Risk Management Strategy

Contents

1. RISK MANAGEMENT FRAMEWORK

1.1 General

Council's risk management framework provides the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation. The two key elements of Council's framework are its Risk Management Policy, which establishes a mandate and commitment for managing risk, and the Risk Management Strategy which details the procedures and processes by which risk management will be implemented within the organisation.

Council understands the importance of an effective risk management framework to help protect key stakeholders from adverse events and support the pursuit of opportunity. Therefore, Council will maintain a risk management framework appropriate to the size, culture and complexity of its operations and environment.

1.2 Risk Management Policy

Council has an adopted Risk Management Policy. This policy "sets the tone" for Council's risk management approach and establishes the risk management responsibilities of the Council, General Manager, EXCOM, Executive Directors, Managers and staff.

This Risk Management Strategy supports the Risk Management Policy by further defining the systems and processes necessary to maintain an effective and efficient risk management framework.

1.3 Risk Management Strategy

This Risk Management Strategy specifies the approach, the management components and resources to be applied to the management of risk. It details the procedures, practices, assignment of responsibilities, sequence and timing of activities to help all people within the organisation manage risk.

The risk management process can be applied to a particular activity, service, process and project, and to part or whole of the organisation.

The Risk Management Strategy also aims to ensure a consistent, proactive and holistic approach that encourages a 'whole of business' or 'enterprise-wide' view of risk rather than managing risk in silos.

1.4 Benefits of Managing Risk

The benefits of a risk aware culture, regular risk management thinking and managing organisation-wide risks will include:

- increased likelihood of achieving objectives;
- better decision-making and planning;
- better identification of opportunities and threats;
- pro-active rather than re-active management;
- more effective allocation and use of resources (human, financial, intellectual);
- improved stakeholder confidence and trust;
- improved compliance with key regulatory requirements;
- improved internal control environment;
- better corporate governance; and
- enhanced communication and reporting of risk.

1.5 Risk Management Parameters

It is important that Council understands its risk taking parameters and articulates its policies and procedures accordingly. Risk parameters are generally expressed in terms of risk appetite and risk tolerance.

Risk appetite is the amount of risk that the organisation wants to take and is willing to accept in pursuit of its objectives. It is the organisation's "comfort zone". It is about knowing where to draw the line between acceptable risks and unacceptable risks and identifying the level of additional controls that are required. Understanding risk appetite is particularly relevant when Council has to make choices that are inherently uncertain such as investment strategy, major outsourcing appointment, major projects and long term strategy formulation.

Whilst risk appetite may vary depending on the importance and complexity of each objective that Council is pursuing and the particular strategies in place to achieve those objectives Council's risk appetite can be summarised as follows:

Council has little or no appetite for known and avoidable operational risks that might impact on the safety and wellbeing of staff and the community, security of Council and public assets, Council's reputation and service delivery. Council acknowledges that it will have to take some calculated risks in order to achieve its strategic objectives. However, in taking such risks Council must consider current financial and human capacity and the potential impact on longer term financial, environmental and social sustainability.

Risk tolerance is the amount of risk an organisation is willing to bear in respect of a particular business line, function or risk type. Ideally, the tolerance is quantified, but in any event is expressed so that relevant management responsibilities are absolutely clear. Risk tolerance is effectively the quantification of Council's risk appetite. Risk tolerance which cannot be expressed in financial terms is more difficult to quantify and needs to be closely assessed as risks are identified and analysed. Council's risk tolerances are detailed in the likelihood and consequence tables appended to this Strategy.

2. RESPONSIBILITIES AND ACCOUNTABILITIES

People, specifically managers who are designated 'risk owners', will play a key role in Council's risk management framework. Key risk management responsibilities are set out below. These responsibilities and accountabilities should be included in staff position descriptions and relevant Committee charters.

The Council is ultimately responsible for adopting and committing to the risk management policy. Responsibilities specific to the risk management framework include:

- reviewing and approving the Risk Management Policy;
- providing feedback to management on important risk management matters/issues raised by management;
- supporting management in communicating the importance and benefits of good risk management to stakeholders;
- fully considering risk management issues contained in Council reports.
- identifying and monitoring emerging risks

The General Manager with the assistance of EXCOM is responsible for leading the development of an enterprise risk management culture across the organisation and ensuring that the Risk Management Policy and Strategy are being effectively implemented. Specifically the General Manager is responsible for:

- where appropriate, reporting known potential risks, emerging risks or major incidents to the Council in a timely manner;
- determining whether to accept or further treat residual risks that are assessed as high or above;
- ensuring that risk management activities are aligned to Council's strategy and objectives; and
- ensuring sufficient funds are available to support effective and efficient management of risks.

EXCOM is responsible for:

- establishing and reviewing the framework for identifying, monitoring and managing significant business risks. This includes periodically reviewing Council's Risk Management Policy and Strategy
- oversight and monitoring of the implementation of Council's Risk Management Strategy
- monitoring the implementation of risk treatment plans
- determining whether to accept or further treat residual risks that are assessed as high or above
- identifying and monitoring emerging risks

Executive Directors are responsible for ensuring that the Risk Management Policy and Strategy are being effectively implemented within their areas of responsibility and determining whether to accept or further treat residual risks that are assessed as medium.

Managers at all levels, are the risk owners and are required to create an environment where the management of risk is accepted as the personal responsibility of all staff, volunteers and contractors. Managers are accountable for the implementation and maintenance of sound risk management processes and structures within their area of responsibility in conformity with Council's risk management framework including:

- identifying, recording and periodically evaluating risks;
- identifying, recording and assessing effectiveness of existing controls;
- implementing and maintaining effective internal controls;
- developing treatment plans to treat higher level risks in a timely manner; and
- maintaining up to date risk registers through quarterly reviews and updates.

Managers are also responsible for supporting good management practices that compliment risk management including:

- complying with and monitoring staff compliance with Council's policies, procedures, guidelines and designated authorities;
- maintaining up-to-date information and documentation for key operational processes; and
- incorporating risk treatment plans into sectional operating plans and Council's Operational Plan and budget as required.

The Corporate Compliance Coordinator is responsible for coordinating the processes for the management of risk throughout the organisation. This may include the provision of advice and service assistance to all areas on risk management matters. Specific responsibilities include:

- ensuring the risk management framework remains relevant and appropriate for Council;
- making recommendations on all aspects of the risk management framework to Management and risk owners;
- providing advice and support to the Council, EXCOM, managers and all staff on risk management matters;
- providing or co-ordinating the delivery of appropriate and relevant training to staff to promote a positive risk, compliance and control culture;
- periodically reviewing key risk management related documents including risk registers, risk profiles, policies, plans, procedures and authorities; and
- reporting quarterly to EXCOM on any risk issues arising from the quarterly risk register review and the current status of key risks, Risk Treatment Plans, incidents and other relevant issues.

All staff, contractors and volunteers are required to act at all times in a manner which does not place at risk the health and safety of themselves or any other person in the workplace. Staff should provide input into various risk management activities. Staff are responsible and accountable for taking practical steps to minimise Council's exposure to risks in so far as is reasonably practicable within their area of activity and responsibility.

All staff must be aware of operational and business risks. Particularly, they should:

- provide input into various risk management activities;
- assist in identifying risks and controls;
- report all emerging risks, issues and incidents to their manager or appropriate officer; and
- follow Council policies and procedures.

3. DOCUMENTATION

Important risk management processes and activities will be documented throughout Council. Documentation is important for the following reasons:

- it gives integrity to the process and is an important part of good corporate governance;

- it provides an audit trail and evidence of a structured approach to risk identification and analysis;
- it provides a record of decisions made which can be used and reviewed in the future; and
- it provides a record of risk profiles for Council to continuously monitor.

3.1 Key documents

Key documents will include:

- Risk Management Policy
- Risk Management Strategy
- Risk Register.
- Risk Treatment Plans

3.2 Maintenance of key documents

Risk documentation including risk registers, written/formal risk assessments, risk/control audits, self-assessments will be maintained in Council's official record keeping system.

These records may be called upon in the management of ongoing treatments, as evidence in incident investigations, in dealing with insurance matters or during other inquiries, and for audit purposes.

Risk management records should be reviewed:

- On handover of responsibilities between managers;
- On assumption of responsibility for a project or program;
- Regularly to match reporting requirements; and
- Whenever operating parameters are subject to major change

4. RISK MANAGEMENT ACTIVITIES, REPORTING AND REVIEW

4.1 Risk Management Framework Review

Documentation including policies, procedures, risk registers and systems relating to the risk management framework will be subject to periodic review. In particular the Corporate Compliance Coordinator is to coordinate a review of the Risk Management Policy every four years (or earlier if there are any material changes in circumstances). The results of the review are to be reported to EXCOM and ultimately the Council. The Corporate Compliance Coordinator must also review the Risk Management Strategy annually and submit the outcome and any recommended changes to EXCOM for adoption.

4.2 Corporate Risk Register Establishment and Review

All managers are required to establish and periodically review risk registers for their areas of the organisation. These risk registers should identify and evaluate key strategic and operational risks that are relevant to the area in question in accordance with the process described in Section 5 of this Strategy. The registers should also identify and evaluate controls in place to manage those risks and identify any required Risk Treatment Plans. Collectively, these registers will form a Corporate Risk Register. The general format of the register is shown in Appendix F.

Each Manager is to conduct a quarterly review of their section's register in conjunction with Council's quarterly performance management process. Managers will be required to sign off that their register has been reviewed and that controls are appropriate. Any changes to the register and/or new or amended risk treatment plans as a result of this review are to be reported to EXCOM by the Corporate Compliance Coordinator. The requirement for a formal quarterly review does not preclude more regular review of risk registers. Regular review of risk registers is encouraged particularly when there are changes in the operating environment and/or new risks are identified.

The risk register review is an integral part of the annual business planning cycle to ensure that:

- risks are identified and assessed in the context of Council's and each Section's current objectives;
- the status of risks and controls is reviewed in conjunction with the review of each section's performance;

- where necessary, risk treatment plans are incorporated into the Operational Plan; and
- where funding is required to implement risk treatment plans that it is incorporated into Council's budget.

4.3 Risk Treatment Plans

Risk owners are responsible for ensuring that actions contained in risk treatment plans (RTPs) are implemented effectively and within agreed timeframes. Action taken is to be recorded in the records system. In addition, Risk Owners are responsible for ensuring that actions contained in RTPs are included in their business plans and where appropriate Council's Operational Plan.

4.4 Risk Status Reports

The Corporate Compliance Coordinator is to coordinate the preparation of a quarterly risk status report to be submitted to EXCOM. The quarterly risk status report will at least contain details of:

- any risk management initiatives undertaken during the previous quarter
- any major incidents that have occurred during the previous quarter
- the major inherent and residual risks facing the organisation and the controls in place to manage those risks
- progress in implementing key risk treatment plans
- any issues that may have arisen as a result of the quarterly risk register review by Managers

4.5 Major Projects, Tenders, Procurement or New Initiatives

Council has implemented a Project Planning framework which includes the requirement for a full risk assessment to be undertaken prior to embarking on any major projects, tenders, procurement activities or other new initiatives. The risk assessment should clearly detail the risks involved and the controls in place (or proposed) to manage those risks. The results of the risk assessment must be included in any report to EXCOM or Council recommending a proposed course of action. The relevant Council Manager is responsible for ensuring that such an assessment is undertaken.

The following checklist is to be used to determine whether a project or initiative requires a formal risk assessment. If the project or initiative will involve:

- The acquisition or development of real property; or
- Significant impact on the community and/or the environment; or
- New expenditure or income in excess of $150,000; or
- Significant impact on Council's ability to achieve key objectives; or
- High potential for fraud, corruption or serious and substantial waste

then a formal risk assessment must be conducted.

4.6 Operational Plan and Annual report

Council's annual Operational Plan must include a section on Risk Management that details proposed risk management activities for the coming year and discusses any key risk management issues. In particular, the Operational Plan should identify key risks that may impact on objectives as well as strategies and controls in place (or proposed) to manage those risks.

Council's annual report must include a section on Risk Management that details risk management activities undertaken during the previous year and any relevant risk management issues.

4.7 Training

All risk owners and other key staff require periodic training in how to implement the risk management process and their responsibilities and obligations under Council's Risk Management Policy and Strategy. General risk management training should be provided to all risk owners and other relevant staff every four years.

In addition, all new staff should be advised of Council's commitment to risk management and their responsibilities and obligations when they commence working for Council. This should generally be done

through a short introduction at Council's induction session followed by a more detailed training session within three months of commencing employment. The training may be delivered internally or externally or by a combination of the two. The Corporate Compliance Coordinator is responsible for coordinating the provision of such training.

4.8 Staff Performance Management

In order to re-enforce accountability and evaluate risk management performance, risk management will be a key component of each Manager's annual performance appraisal. Risk management responsibilities and accountabilities should also be included in staff position descriptions.

4.9 Other Risk Assessment Activities

In order to manage specific risks, Council has in place a range of risk assessment processes. For example, in order to manage the safety risks specific to particular works and activities Council has a safety management system which requires a systematic and detailed assessment of safety hazards and risks. These specific risks do not need to be replicated in the corporate risk register nor do they need to be assessed against the corporate risk matrix if there are specific matrices and criteria in place for the particular type of risk in question. However, the process for assessing such risks must be generally consistent with the process described in this Strategy. This relationship is depicted in the following diagram:

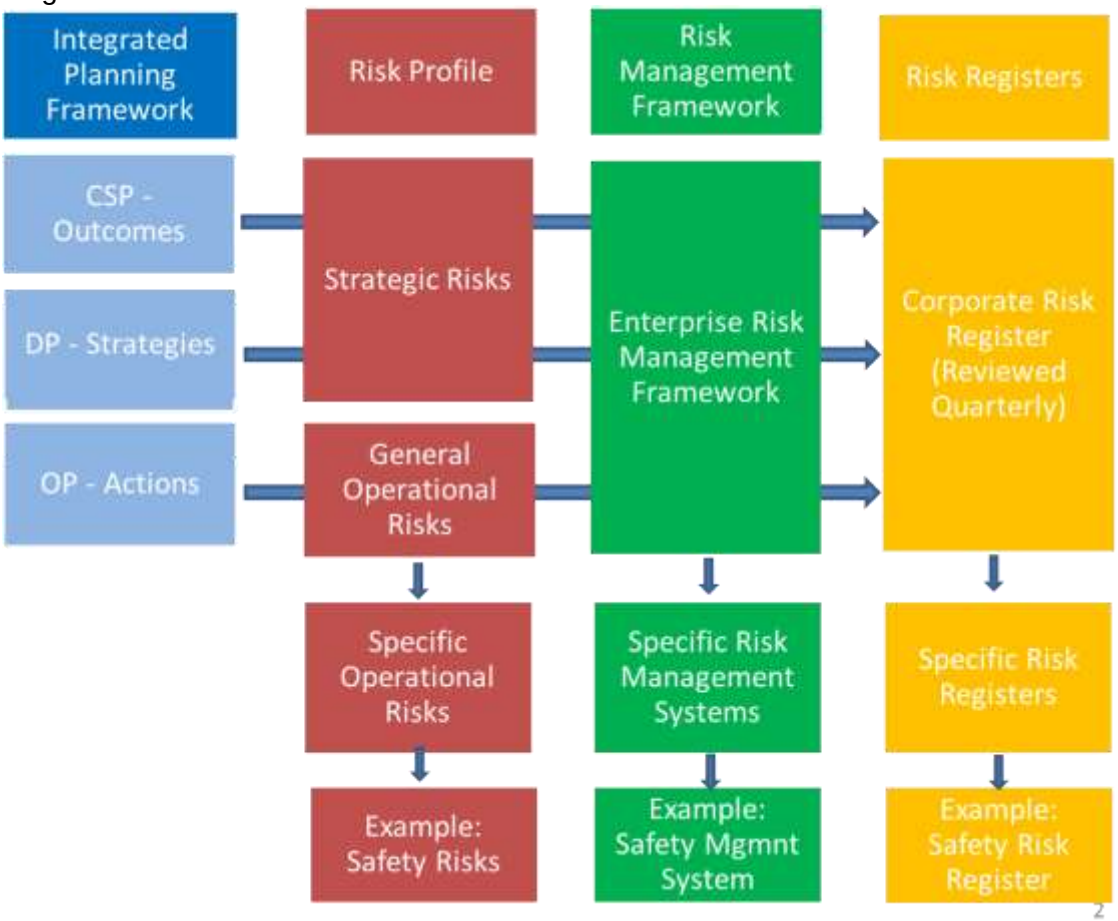

Figure 1: Relationship between risk registers and corporate objectives

4.10 Communication

Ongoing communication of the importance of risk management and the role of staff in managing risk is critical to success of the risk management framework. Accordingly, the Corporate Compliance Coordinator will ensure that relevant risk management information is communicated to staff on a regular basis. This may be done through a range of mediums including the Council intranet, newsletter and e-mail system.

4.11 Summary of Actions, Reviews and Reports

Appendix A summarises the key actions, reviews and reports required by Council's Risk Management Strategy. It details who is responsible for each activity and the required timing.

5. THE RISK MANAGEMENT PROCESS

5.1 Risk Management Process

Council will utilise the Australian and New Zealand Risk Management Standard AS/NZS ISO 31000:2009 to manage risks. This is a structured and proactive approach that can be applied organisation-wide to support management of strategic and/or operational risks.

Under this approach, there are five key stages to the risk management process.

1. Communicate and consult - with internal and external stakeholders
2. Establish context - the boundaries
3. Risk Assessment - identify, analyse and evaluate risks
4. Treat Risks – implement and assess controls to address risk
5. Monitoring and review – risk reviews and audit

Refer to figure 2 below for an illustration of the AS/NZS ISO 31000:2009 risk management approach.

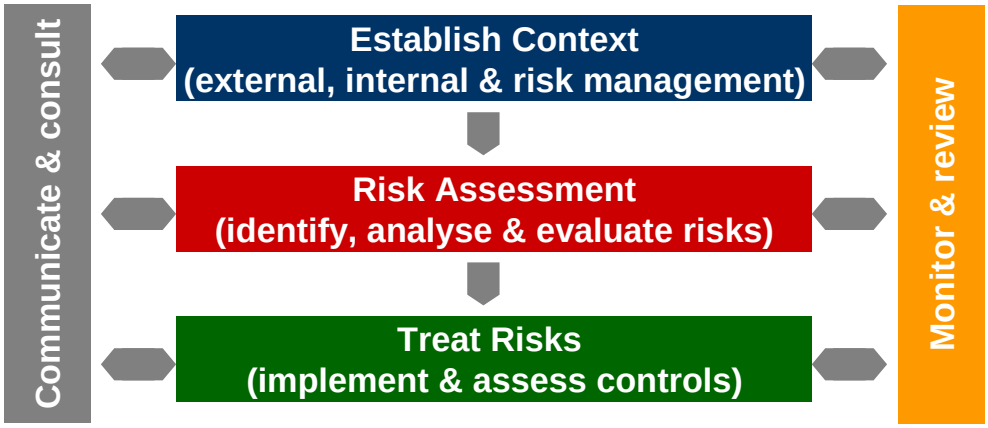

Figure 2: Our risk management approach using AS/NZS ISO 31000 Risk Management Standard

5.1.1 Establish context

Establishing the context of risk management at Council is the foundation of good risk management and vital to successful implementation of the risk management process.

Context is typically established by the risk leadership team and involves setting boundaries around the depth and breadth of risk management efforts to help Council stay focused and align the risk management framework to relevant matters.

Important considerations when determining context include:

- Council's external environment – social factors, demographics, economic, environmental.
- Council's stakeholders – residents, rate payers, customers, regulators, employers, politicians, media, insurers, service providers, staff and volunteers.
- 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. Section 1.5 of this Strategy summarises Council's general appetite for risk.

5.1.2 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 risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives.

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

- Strategic risks;
- Operational risks;
- Financial risks;
- Reputational risks;
- Legal and Regulatory risks;
- Business disruption;
- Human risks; and
- Environmental 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
- Personal experiences
- Expert judgement
- Periodic working 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

5.1.3 Risk Analysis

Once risks have been identified, they are then analysed. Risk analysis involves consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur. At this point, no consideration is given to existing controls. The following risk criteria should be used as a guide when analysing risks.

The likelihood of occurrence is the probability of an event occurring. When considering the likelihood of a risk, you need to consider both the probability and frequency of occurrence. Council will utilise the likelihood ratings shown in Appendix B.

The consequence assessment is the effect or impact of the risk event. It is measured both financially (in terms of profit/loss or balance sheet impact) and operationally (human & physical). Council will utilise the consequence ratings shown in Appendix C.

Inherent risk is the overall raw risk. It is determined by combining the likelihood and consequence ratings. Ultimately, the level of inherent risk will determine how a risk is treated. The table shown in Appendix D depicts the inherent risk levels that will be used by Council.

5.1.4 Risk Evaluation

Risk evaluation involves comparing the level of risk found during the analysis process against Council's known priorities and requirements.

Any risks accorded too high or too low a significance are adjusted, and documented accordingly. The output of the risk evaluation is a prioritised list of risks for further action.

5.1.5 Risk Treatment

Risk treatment involves selecting one or more options for modifying risks, and implementing those options. It involves identifying and evaluating existing controls and management systems to determine if further action (risk treatment) is required.

Existing controls are identified and then assessed as to their level of effectiveness. Council will utilise the control effectiveness ratings shown in Appendix E.

Residual risk is the level of risk after considering existing controls. It is determined by applying the effectiveness of existing controls to inherent risk. The table in Appendix D - Risk Level Ratings (see above) should also be used to determine the level of residual risk.

Ultimately, the level of residual risk will determine how a risk is treated.

Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. The options can include the following:

a) avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
b) taking or increasing the risk in order to pursue an opportunity;
c) removing the risk source;
d) changing the likelihood;
e) changing the consequences;
f) sharing the risk with another party or parties (including contracts and risk financing); and
g) retaining the risk by informed decision.

When a residual risk is assessed as Medium or High and a decision is made that the risk is not acceptable, a Risk Treatment Plan must be developed in order to reduce the risk to an acceptable level within an appropriate time frame.
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.

For the various levels of residual risk, the following process must be followed:
High or Extreme:
Requires immediate risk treatment as the potential risk exposure could be devastating to the organisation. The existence of a High or Extreme residual risk and any proposed action to further treat such a risk must be reported to the General Manager and/or EXCOM for consideration as soon as possible. EXCOM and/or the General Manager must determine whether the proposed risk treatment, including the time frame for implementation, is acceptable. In some rare cases EXCOM and/or the General Manager may determine to accept a High or Extreme residual risk without further treatment where the cost of treatment exceeds the benefit and the objective being pursued is considered critical. In such cases, the reason for accepting the risk without further treatment must be documented.

Medium:
May require action at some point in the near future, as it has the potential to be damaging to the organisation. Medium risks and any proposed action to further treat such risks must be reported to the General Manager, relevant Executive Director and/or EXCOM for consideration as soon as practicable. The General Manager, relevant Executive Director and/or EXCOM must determine whether the proposed risk treatment, including the time frame for implementation, is acceptable. Medium risks may be accepted in some circumstances, most likely when the cost of further treatment exceeds the benefit. In such cases, the reason for accepting the risk without further treatment must be documented.

Low:
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.

5.1.6 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 plans will be assessed to ensure changing circumstances do not alter risk priorities. Feedback on the implementation and the effectiveness of the Risk Management Policy and Strategy will be obtained from the risk reporting process, internal audits and other available information.

Council has adopted the Australian Business Excellence Framework (ABEF) as its framework for internal audit and continuous improvement. Risks and controls will be monitored and tested regularly in line with their significance through the ABEF.

Key Risk Indicators (KRIs) may be developed to monitor risks on an ongoing basis. KRI's are operational in nature and should be determined by the risk owner once risks and their causes have been identified.

5.1.7 Communication and Consultation

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. Staff 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.

5.1.8 External Specialists

Given the size and risk profile of Council, external specialists may be needed from time to time to assist the organisation in evaluating and treating risks.

6. Appendix

Appendix A – Summary of Key Risk Management Activities

Action	Description	Responsibility	Timing
Review RM Policy	Review the currency and effectiveness of Council's Risk Management Policy	Council to adopt (review to be coordinated by Corporate Compliance Coordinator)	Every four years
Review RM Strategy	Review the currency and effectiveness of Council's Risk Management Strategy	EXCOM to adopt (coordinated by Corporate Compliance Coordinator)	Every year in November
Review Risk Register	Review risks and controls contained in Council's corporate risk register and identify new or emerging risks	All Managers (risk owners) to complete review and report as part of the Quarterly Performance Management process	Every quarter in conjunction with Quarterly Performance Management Process
Include Risk Treatment Plans in Operational Plan	Ensure that actions required by Risk Treatment Plans (RTP) are incorporated into the Operational Plan	All Managers (risk owners) (Corporate Compliance Coordinator to oversee)	Every year/ quarter in conjunction with Operational Plan development/ review
Implement Risk Treatment Plans	Implement actions contained in risk treatment plans (RTP)	Risk Owners	As identified in the RTP
Risk assessments for major projects/ initiatives	Conduct risk assessments as required for major new or altered activities, processes or events	Relevant Manager/ Risk Owner (Corporate Compliance Coordinator to assist)	Prior to deciding to proceed with new project/ initiative
Risk Status Report	Identify and review, by exception, any risk issues arising from the Quarterly risk register review and the current status of key risks, RTPs, incidents and other relevant issues	EXCOM (co-ordinated by Corporate Compliance Coordinator)	Quarterly

Annual Report	Detail risk management activities undertaken during the previous year and any relevant risk management issues.	Corporate Compliance Coordinator	Annual
Operational Plan	Identify key risks that may impact on objectives as well as strategies and controls in place (or proposed) to manage those risks.	Managers/ Risk Owners (overseen by Corporate Compliance Coordinator)	Annual
Training	Ensure risk owners and other staff are aware of the risk management process and their obligations	Corporate Compliance Coordinator	Refresher for all Managers and Risk Owners every four years. Introduction for all new staff at induction with more detailed session within three months of commencing.
Staff Performance Review	Ensure risk management performance of managers is assessed on a regular basis	Manager Human Resources	Annual
Communication	Ensure staff are aware of relevant risk management issues and have access to risk management tools.	Corporate Compliance Coordinator	Ongoing

Appendix B - 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 or more. Less than 10% chance of occurring.
2	Unlikely	The event could occur in some circumstances. No past event history.	Once every 20 years. Between 10% and 30% chance of occurring.
3	Possible	The event may occur sometime. Some past warning signs or previous event history.	Once every 5 years. Between 30% and 70% chance of occurring.
4	Likely	The event will probably occur. Some recurring past event history	Once a year. Between 70% and 90% chance of occurring.
5	Almost Certain	The event is expected to occur in normal circumstances. There has been frequent past history.	Several times a year. Greater than 90% chance of occurring.

Appendix C – Consequence Ratings

Impact on Objectives		Area	Impact on Specific Business Areas (To guide assessment)
Extreme	Most objectives can no longer be achieved. Complete revision of long term business model required.	Financial	>$2m recurrent reduction in operating budget, one off loss of > $5m, Inability to pay staff and creditors
		Environmental	Very serious irreversible damage to environment and/or multiple sites or ecosystems, prosecution of Council
		Reputation	Sustained negative local or national media coverage, widespread public outcry and loss of trust in Council, damage to reputation that takes many years to repair, investigation resulting in prosecution or sacking of Council
		Service Disruption	Key activities and essential services disrupted for over 14 days
		Human	Major negative impact on staff morale, loss of life, major repeated breaches of WHS legislation, prosecution, successful class action
High	A number of significant business objectives can no longer be achieved.	Financial	$1m-$2m recurrent reduction in operating budget, one off loss of $3m- $5m, delayed payment to staff and creditors
		Environmental	Significant long term impact on built & natural environment, investigation of Council with adverse findings
		Reputation	Significant adverse media at state level, significant & well publicised outcry from residents, long story life
		Service Disruption	Key activities disrupted for between 7 and 14 days
		Human	Major localised impact on staff morale, breach of legislation, lost time injuries requiring major medical treatment, multiple insurance claims
Medium	Some important business objectives can no longer be achieved.	Financial	$250k-$1m recurrent reduction in operating budget, one off loss of $1m-$3m
		Environmental	Serious medium term effects on built & natural environment from single incident(eg one off pollution spill)
		Reputation	Concerns from broad section of residents, major local media coverage (short duration),
		Service Disruption	Key activities disrupted for between 3 and 7 days
		Human	Minor breach of safety legislation, short duration lost time injury requiring minor medical treatment, one off insurance claims
Minor	Some reprioritisation of resources to enable business objectives to be achieved.	Financial	$50k-$250k recurrent reduction in operating budget, one off loss of $250k-$1m
		Environmental	Short term effects on built & natural environment, damage to a single property or parcel of land, breach of policy
		Reputation	Heightened concerns from narrow group of residents, some media concern, opportunistic fraud by single staff member
		Service Disruption	Some Council activities disrupted for up to 3 days
		Human	Some short term impact on staff morale, minor injuries or illness from normal activities treated by first aid
Very	Little or no impact on	Financial	<$50k recurrent reduction in operating budget, one off loss of <$250k
		Environmental	Minor effects on built & natural environment, breach of guidelines, perception of damage
		Reputation	One off insignificant adverse local media or public complaints

	business objectives.	Service Disruption	Usual scheduled interruptions, unscheduled interruptions for less than 4 hours
		Human	Localised raising of concerns by staff, incident and/or ‘near miss’

Appendix D – Risk Rating Matrix

	Consequence				
Likelihood	1 Very Low	2 Minor	3 Medium	4 High	5 Extreme
5 Almost Certain	Medium	Medium	High	Extreme	Extreme
4 Likely	Low	Medium	Medium	Extreme	Extreme
3 Possible	Low	Low	Medium	High	Extreme
2 Unlikely	Low	Low	Medium	Medium	High
1 Rare	Low	Low	Low	Medium	Medium

Appendix E – Control Effectiveness Ratings

Rating	Effectiveness	Description	Quantification
0	Not Effective	The control does not address risk	0%
1	Slightly Effective	The control is not reliable as it is not well designed, documented and/or communicated.	1-20% effective
2	Somewhat Effective	Control may be reliable but not very effective as control design can be improved.	21-40% effective
3	Reasonably Effective	Control is reliable but not effective as documentation and/or communication could be improved.	41-60% effective
4	Mostly Effective	The control is mostly reliable and effective. Documentation exists but can be better communicated.	61-80% effective
5	Very Effective	Control is reliable and effective. Fully documented process and well communicated.	81-100% effective

Appendix F - Risk Register Template

Location	Risk No	Risk Description	Likelihood	Consequence	Inherent Risk	Control Description	Control Effectiveness	Control Status	Residual Risk	Residual Risk Acceptable ?	Details of Risk Treatment Strategy Required

Appendix G- Risk Management Glossary
Adapted from AS/NZS ISO 31000

communication and consultation	continual and iterative processes that an organisation conducts to provide, share or obtain information and to engage in dialogue with stakeholders and others regarding the management of risk stakeholder person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity
consequence	outcome of an event affecting objectives
control	measure that is modifying risk
establishing the context	defining the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy
external context	external environment in which the organisation seeks to achieve its objectives
internal context	internal environment in which the organisation seeks to achieve its objectives
level of risk	magnitude of a risk, expressed in terms of the combination of consequences and their likelihood
likelihood	chance of something happening
monitoring	continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected
residual risk	risk remaining after risk treatment
review	activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives
risk	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 attitude	organisation's approach to assess and eventually pursue, retain, take or turn away from risk
risk aversion	attitude to turn away from risk
risk criteria	terms of reference against which the significance of a risk is evaluated
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 finding, recognizing and describing risks
risk management	coordinated activities to direct and control an organisation with regard to risk
risk management framework	set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation
Risk Management Strategy	scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk
risk management policy	statement of the overall intentions and direction of an organisation related to risk management
risk management process	systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk
risk owner	person or entity with the accountability and authority to manage the risk
risk profile	description of any set of risks
risk source	element which alone or in combination has the intrinsic potential to give rise to risk event
risk treatment	process to modify risk