

Risk Management Framework

First Approved	19 October 2015 - Resolution Ref: ACM15398
Review Frequency	4 yearly or as required
Status	LGA Recommended
Last Reviewed	January 2018 – administrative review 16 March 2020 – Resolution Ref: ACM20528 (administrative update) 17 July 2023 – Resolution Ref: C23278
Next Review Due	July 2027
File Number	18.87.003 / CD20231895
Responsible Division	Office of the CEO
Related Documents	Alexandrina Council Risk Management Policy AS ISO 31000:2018 Risk Management Guidelines SA HB:436.1:2020 Risk Management Guidelines – companion to AS ISO 31000:2018, Part 1: Boards and executives Alexandrina Council Risk Register Return to Work SA Code of Conduct for Self-Insured Employers Work Health Safety and Return to Work Policy
Applicable Legislation	<i>Local Government Act (SA) 1999, s.122, 125 & 134</i> <i>Work Health and Safety Act 2012</i> <i>Civil Liability Act 1936</i> <i>Local Government (Financial Management Regulations) 2011</i> <i>State Records Act 1997</i> <i>Commonwealth Privacy Act 1988</i> <i>Freedom of Information Act 1991</i>

Purpose

This Framework outlines the requirements and processes supporting Alexandrina Council's Risk Management Policy to create and protect value by improving performance, encouraging innovation and supporting the achievement of strategic objectives.

This Framework:

- Aligns with the objectives of the Risk Management Policy;
- Establishes roles and responsibilities for managing risk;
- Documents a standardised, formal and structured process for assessment, evaluation, treatment and monitoring of identified risks;
- Encourages innovation by integrating risk management into the strategic and operational processes throughout the organisation;
- Will assist Council in maximising its opportunities, whilst minimising negative impacts identified during the risk management process;
- Establishes the process for all risks outside the risk appetite, when defined, to be escalated to the appropriate level and for additional treatment options to be implemented.
- Sets out reporting protocols for relevant risk information to be provided to Council, Internal Audit Group, the Executive and throughout the organisation; and
- Will support the development of a continuous improvement culture by integrating risk management processes throughout the organisation.

Risk Management Principles

The Australian standard for Risk Management Guidelines (AS ISO 31000:2018) describes risk as:

“...the effect of uncertainty (either positive, negative or both) on objectives...”

The goal is not to eliminate all risks, but rather to manage risks involved in delivering Alexandrina Council's functions and services and to create and protect value for stakeholders and community.

AS ISO 31000:2018 is based on the following eight principles, which underpin this Framework and guide how risk is managed across the organisation:

Integrated	An integral part of all organisational processes
Structured and comprehensive	Contributes to efficiency and to consistent and comparable results
Best available information	Based on historical and current information, as well as on future expectations, taking into account any limitations associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders.
Customised	Aligns with the internal and external context related to our objectives
Human and cultural factors	Recognises that the behaviour and culture can significantly influence the achievement of objectives
Inclusive	Requires appropriate and timely involvement of stakeholders to enable their knowledge, views and perceptions to be considered.
Dynamic	Anticipates, detects, acknowledges and responds to changes in Member's internal and external contexts that result in new risks emerging and others changing or disappearing
Continual improvement	Learning and experience drives continuous improvement

Risk Management Framework



Leadership and commitment

Alexandrina Council and the Executive will demonstrate a clear commitment to managing risks throughout the organisation by:

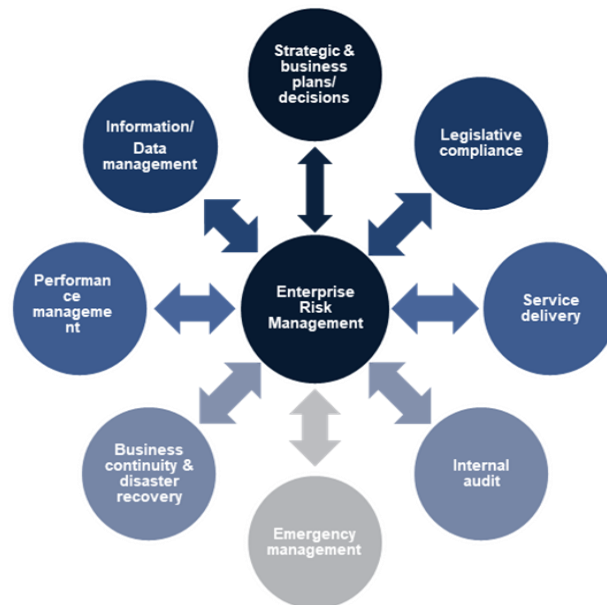
- Developing and implementing a risk management policy, framework and supporting tools and processes;
- Allocating appropriate resources to implement, monitor and improve the effectiveness of risk management;
- Ensuring that staff, contractors, volunteers and other relevant stakeholders have the appropriate skills and knowledge to deal with risk;
- Allocating and upholding accountability with respect to risk management and ensuring it is understood; and
- Ensuring compliance with legislative and contractual obligations and policy requirements.

Integration

This Framework provides the methods and processes Alexandrina Council utilises to manage risks and identify opportunities throughout the organisation.

Governance guides the direction of the organisation and provides the rules, processes and practices necessary to achieve objectives. Management structures that define risk management accountability and oversight roles across the organisation are critical to achieving sustainable performance and long-term viability.

Risk Management is not just about the risk assessment process nor is it a stand-alone discipline. In order to maximise benefits and opportunities, it requires integration throughout the organisation, as follows:



Corporate Risk Management

Corporate risk management encompasses strategic, operational and project risk management.

Strategic risks are identified by reference to both the external environment and strategic objectives. Strategic risks are monitored by the Executive, Internal Audit Group and Council, with all identified risks captured in the Risk Register and recorded within the record management system.

Operational Risks arise from day-to-day functions and operations to deliver core services. Operational risks are monitored by Department Managers.

Project Risks are the uncertain events or conditions that have potential to impact either positively or negatively on project objectives. Project risks are monitored by the project manager and reported to the Executive and the Council, (where the project is of strategic significance.)

Strategic planning and decision making

Strategic and business planning, (which includes long-term financial planning and annual budgeting,) must adequately consider the risks inherent in setting and pursuing objectives and the effectiveness of systems that are in place to manage and communicate those risks.

Risk management is integrated into governance structures, including decision making, which is supported by incorporating risk analysis into Council and committee reports, where there is a potential impact on the achievement of strategic objectives or on the wider community.

Legislative compliance

The Local Government Act (SA) 1999 applies to the functions of Councils and Prescribed Bodies in South Australia, however, due to the diversity of functions provided, a range of other Acts, Regulations and Codes of Practice and Standards also apply. In essence, Council should ensure the areas of highest compliance risk are addressed with greater rigor. Risk is considered in determining controls established (or which need to be established) to

ensure compliance with applicable Legislative and Regulatory obligations (i.e. the higher the inherent risk for the obligation, the more important the controls required).

Alexandrina Council has implemented a Work Health and Safety (WHS) management system to manage hazards and risks to workers and members of the public, in accordance with the WHS Act (SA) 2012 and Return to Work SA's Performance Standards for Self Insurers.

Service delivery

Risk exposures vary according to the functions, facilities and services provided and these will inevitably change over time. Alexandrina Council's planning processes address both the risks associated with provision of functions, facilities and services, (such as capacity and resources,) and risks arising from their delivery, (such as public safety and community reaction). Specific risk assessments should be undertaken where required.

Internal audit

Internal audit is an independent, objective assurance activity designed to add value and improve the organisation's operations. It provides a systematic, disciplined approach to evaluating and improving the effectiveness of risk management, control and governance processes. Internal Audit projects should be undertaken on areas of highest inherent risk. The process of internal audit may result in the identification of new risks or more effective treatments for existing risks.

In addition to its own internal audit program, Alexandrina Council engages an independent auditor to undertake an audit of internal controls as required by Section 125 of the Local Government Act (SA) 1999 and Part 6, Regulation 19 of the Local Government (Financial Management Regulations) 2011.

Emergency Management

Alexandrina Council plans for, and undertakes, prevention, preparedness, response activities to support its community in the event of emergencies and natural disasters. This process includes alignment and co-operation with lead agencies and other Councils in the state as well as providing information and training for workers to protect them from harm whilst responding to emergencies and natural disasters.

Business Continuity Plan & Information Technology Disaster Recovery Plan

Alexandrina Council is committed to ensuring that time-critical business functions continue after a business interruption and has developed the following plans, taking into consideration reasonably foreseeable risks and their potential impact on achievement of objectives:

- a) The Business Continuity Plan (BCP), which is designed to manage risk by limiting or reducing the impact of a disruption, (such as severe weather event or loss of key personnel), and enable the resumption of critical business functions/services following a disruption; and
- b) The Information Technology Disaster Recovery Plan (DRP), which is intended to protect and recover information technology infrastructure and data in the case of a disruptive event, (such as cyberattack or damage to/loss of infrastructure,) by defining actions to be taken before, during and after an event.

Performance Management

Both risk management and performance management start with the establishment and communication of corporate goals and objectives and development of strategies which are then cascaded throughout the organisation. Appropriate measures and reporting structures will be put in place to monitor the effectiveness of risk management processes, which will in turn assist in identifying gaps and emerging risks.

Information/Data Management

Not only is it critical to the achievement of objectives that data and corporate knowledge is retained, there are regulatory requirements to do so, (e.g. compliance with the State Records Act 1997, Commonwealth Privacy Act 1988 and Freedom of Information Act 1991.)

Alexandrina Council's records may be vulnerable to cyberattack, malicious intent or unauthorised release, should appropriate risk mitigation strategies not be in place.

Roles and responsibilities

The following roles and responsibilities ensure a transparent approach to managing risk within Alexandrina Council:

Roles	Responsibilities
Council	<ul style="list-style-type: none">• Set the organisation's policy for managing risk• Give adequate consideration to risks when setting objectives and making decisions• Ensure the organisation has the structures and processes in place to support decision making and management of risk• Set an appropriate governance structure for risk and risk management including the Internal Audit Group and delegations• Require the CEO to demonstrate that the framework for managing risk is effective and appropriate• Require the CEO to provide information to allow the Council to understand the risks that may have material impacts on achievement of the organisation's objectives• Consider recommendations from the Internal Audit Group relating to strategic risks or any other risk matter
Internal Audit Group	<ul style="list-style-type: none">• Review reports from Executive and auditors to ascertain the adequacy of controls that have been implemented• Review and recommend endorsement of the criteria contained within the Risk Management Framework and associated documents• Providing assurance to and assisting Council to ensure risk management is embedded in Alexandrina Council's governance processes• Receive regular risk reports both at the Strategic and Operational level, discuss strategic and emerging risks, controls and treatments and provide comment as appropriate.

Roles	Responsibilities
Chief Executive Officer (CEO)	<ul style="list-style-type: none"> Promote a strong risk management culture by providing firm and visible commitment to risk management including ensuring appropriate accountability for the management of risk As a member of the Executive, review and endorse the Risk Management Framework Develop and implement a framework that delivers a consistent approach to risk management by allocating resources and assigning authority, responsibility and accountability at appropriate levels within the organisation Provide overall risk management leadership and maintenance of a risk culture, embedded into decision-making. Ensure Executive have the necessary knowledge and skills to effectively fulfil their risk management responsibilities Regularly review strategic and operational risks and maintain an understanding of the environment in which the organisation operates, the risks it faces and the effectiveness of its controls Ensure compliance with legislative and contractual obligations and policy requirements Lead responsibility for Strategic Risks (and Executive) Motivate people to think about taking calculated risks for rewards
Executive	<ul style="list-style-type: none"> Commitment to, and promotion of, the risk management policy and framework Review and endorse the criteria contained within the Risk Management Framework Monitor the organisation's overall risk profile and mitigation strategies; Identify new and emerging strategic risks. Ensure that risk management is embedded into all functions and activities, including decision making Empower staff (and employ a 'no-blame' culture) to be actively involved in identifying, assessing, and managing risk; including motivating staff to think about taking calculated risk for reward (in accordance with the Risk Appetite Statement once defined). Ensure appropriate controls and/or treatments are established, maintained and monitored for each strategic risk assigned to them. Ensure that risks that cannot be treated immediately are recorded on the risk register and that there is ongoing and regular review of the risk register, (including follow up and close out of overdue risk treatments)

Roles	Responsibilities
	<ul style="list-style-type: none"> • Ensure that staff, contractors, volunteers and other relevant stakeholders have the appropriate skills to be actively involved in managing risk • Provide performance management arrangements that support the desired approach to managing risk • Promote a proactive risk culture in accordance with business management initiatives • Collectively review strategic risks and consider emerging risks, prior to Internal Audit Group • Ensure compliance with legislative and contractual obligations and policy requirements and activities, including decision making
Risk Management Coordinator	<ul style="list-style-type: none"> • Provide guidance and assistance to Executive Management Team and staff in relation to the application of this framework • Develop and maintain the Annual Risk Action Plan • Support the Chief Executive Officer, Executive and Managers in the discharge of their risk management responsibilities and as a part of decision-making. • Facilitate the development and maintenance of the Strategic Risk Profile • Maintain the Risk Management Policy and Framework to ensure its currency and relevance • Maintain the Risk Register and reporting timeframes as required • Ensuring relevant risk information is recorded in the Risk Register and reported and escalated to the Management Team or cascaded to employees, as relevant
Employees, Volunteers & Contractors	<ul style="list-style-type: none"> • Understand the risk management processes that apply to their area of work • Identify, evaluate, report and manage, (or escalate,) risks relating to daily activities and projects

Risk Management Process

Although the risk management process is often presented as sequential, in practice it is dynamic as illustrated in the AS ISO 31000:2018 Risk management – guidelines:

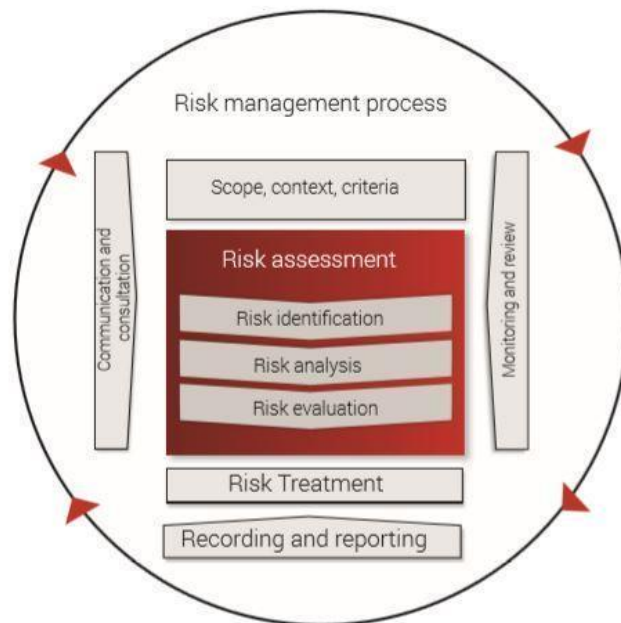


Diagram source: Standards Australia Limited, AS ISO 31000:2018 Risk management – guidelines, SAI Global Limited, Sydney, 2018. © Standards Australia Limited. Copied by JLT Risk Solutions Pty Ltd with permission of Standards Australia and Standards New Zealand under Licence 1811-c079.

Communication and Consultation

Establishing a communication and consultation plan with stakeholders is critical to the success of the risk management process. Alexandrina Council will engage with stakeholders throughout the risk management process.

Scope, context and criteria

Defining the scope

Because the risk management process is applied at different levels throughout the organisation, it is important to define the scope and its alignment with the organisation's objectives. This should include consideration of:

- Goals and objectives of risk management activities;
- Proposed outcomes and timing;
- Responsibilities and accountabilities for the risk management process;
- Processes, activities and projects and how they may interact with other processes, activities and projects;
- How effectiveness and/or value will be measured and monitored; and
- Availability of resources to manage risk.

Defining the context

- Defining the context is important because
 - Risk management takes place in the context of achieving objectives and undertaking activities; and
 - Organisational factors can be a source of risk.
- The context should reflect the specific environment of the activity to which the risk management process is to be applied.

Defining risk criteria

Risk criteria are used to evaluate the significance of risk and are reflective of Alexandrina Council's values, objectives and resources and the views of its stakeholders. Agreed risk criteria will be established through consultation with the Executive, CEO, and Internal Audit Group.

Risk Assessment

Risk Identification

The aim of risk identification is to develop an inclusive list of reasonably foreseeable events that may occur that - if they do - are likely to have an impact on achievement of objectives.

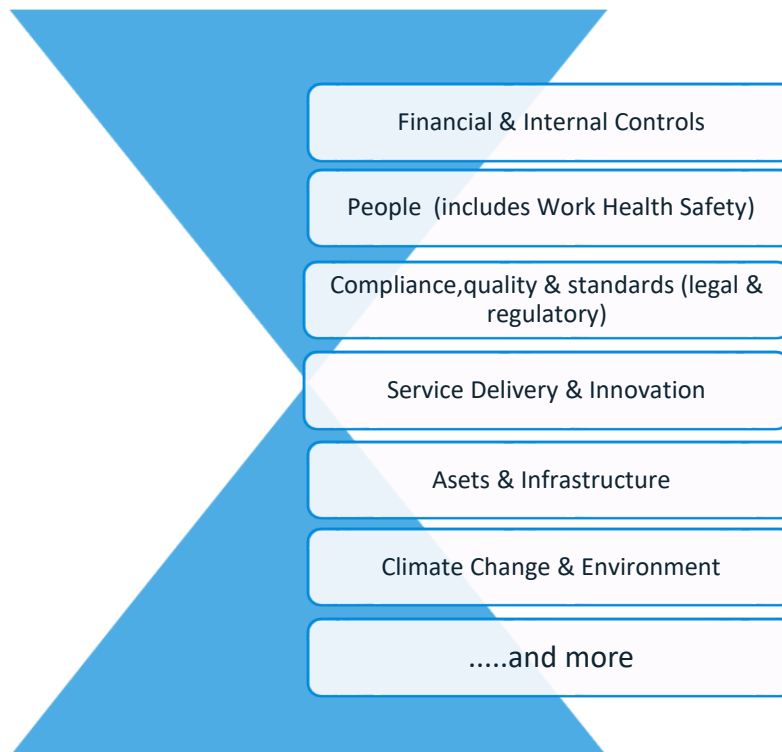
Alexandrina Council identifies, assesses and treats risk in the following three risk types:

Strategic	Risks associated with high-level strategic objectives that are articulated in Strategic, Annual Business and Asset Management Plans. Strategic risks may affect the achievement of Councils corporate objectives. In other words, they may prevent the organisation from achieving its strategic objectives.
Operational	Risks associated with departmental functions and daily operations to deliver core services.
Project	Risks associated with Project Management that will affect milestones or outcomes connected to delivering a specific project.

Risk identification naturally flows on from the context discussion and is a process of formally documenting the effects of uncertainty on objectives.

The aim is to generate a list of risks based on those impacts or events. During the identification process, there are a number of questions that need to be asked to capture the information required:

What might happen/ what could go wrong? What is the cause? How does this affect the objective? After a risk is identified, it may be categorised and captured in the Risk Register in accordance with the following categories:



The process of risk identification must be comprehensive as risks not identified are by nature excluded from further analysis. Care must be taken to identify and define risks, rather than causes or consequences.

Risk Analysis

Risk analysis involves developing an understanding of a risk. This involves considering the causes and sources of the risks, their positive and negative events, and the likelihood that the consequences will occur.

Risk analysis specifically requires identifying, measuring and mitigating various risk exposures or hazards:

- What is the cause/source of the risk?
- What are the positive and/or negative consequences should the risk occur?
- How likely is it that the risk will occur?
- What is the inherent risk rating (risk rating **before** considering existing controls)?
- What controls are currently in place to mitigate the risk and how effective are they?
- What is the controlled risk rating (risk rating **after** considering existing controls)?

The inherent and controlled risk ratings are determined by applying the likelihood and consequence identified during the risk analysis to the Risk Consequence Matrix. (Appendix 1)

Risk Ratings

A “risk rating” can be determined by combining the estimates of effect (consequence rating) and cause (likelihood rating). The risks are to be assessed against all consequence categories; and the highest consequence rating will be used. The following risk ratings are used:

- Residual risk rating, being the level of risk with the controls that are currently in place, operating as they are; and
- Treated risk rating, being the level of risk once further and additional controls are added to reduce the consequence and/or likelihood, (i.e. the forecast level of risk remaining after risk treatment).

Risk Evaluation

The purpose of the risk evaluation is to determine the significance of the risk, based on the outcomes of the risk analysis, and determine which risks require treatment.

This stage of the process will determine whether a risk is acceptable or unacceptable. If the risk is accepted, no further risk treatment is required, however still requires the maintenance of existing controls.

Reasons for deeming a risk to be acceptable include:

- The likelihood and consequence of the risk being so low that specific treatment is considered unnecessary.
- The degree of control to mitigate the risk.
- The risk being such that there is no treatment available.
- The cost of treating the risk outweighing the benefits.

Risks deemed to be unacceptable require treatment options to be implemented to reduce the threat or exploit the opportunity. These risks should be prioritised on the relevant risk register for subsequent management action and reviewed by the Internal Audit Group.

Any outcome from an evaluation process should be recorded, communicated and validated through appropriate levels of the directorate.

Risk Escalation

When a risk has been identified or reassessed, the following table provides guidance on the action to be taken for each risk rating level:

Risk level	Managing risk – priority rating
Extreme	<p>Add risk to Strategic Risk Register; Escalate risk issue immediately to CEO</p> <p>CEO to:</p> <ul style="list-style-type: none">• Refer risk to risk owner• Identify and develop treatment strategies for immediate action• Monitor and review actions/strategies• Inform the next meeting of the Council or Internal Audit Group of the risk issue, the actions taken to mitigate the risk and the outcome (or current status)• Consider cessation/suspension of the activity giving rise to the risk until such time as CEO/Management Team authorises its continuation and/or whilst other risk treatment strategies are being developed/implemented

Risk level	Managing risk – priority rating
High	<p>Add risk to Risk Register</p> <p>Escalate risk issue to member of Executive or Risk Management Coordinator</p> <p>Member of Executive or Risk Management Coordinator to:</p> <ul style="list-style-type: none"> • Refer to relevant risk owner • Identify and develop treatment strategies with appropriate timeframes • Monitor and review actions/strategies to manage risk to an acceptable level • Inform the next meeting of the Internal Audit Group or Executive, (as relevant) of the risk issue, the actions taken to mitigate the risk and the outcome or current status
Moderate	<p>Add risk to Risk Register</p> <p>Escalate risk to department manager</p> <p>Department manager to coordinate with relevant work group to:</p> <ul style="list-style-type: none"> • Identify and develop treatment strategies with appropriate timeframes • Monitor and review actions/strategies to manage risk to an acceptable level
Low	<p>Undertake localised risk management & actions (if required)</p> <p>Review within the department parameters and routine procedures</p>

Risk Treatment

Risk treatment involves selecting one or more options for modifying the likelihood and/or consequence of risks, and implementing those options. Once implemented, treatments provide or modify the controls. An action should be implemented to treat certain risks. Appropriate risk treatment options should have regard to the organisation's objectives, risk appetite, risk criteria and available resources. Justification for risk treatment is broader than solely economic considerations and should take into account all of Council's obligations, voluntary commitments and stakeholder expectations.

Risk treatment priorities

Alexandrina Council has determined that it will prioritise treatment of risks in the following order:

- Strategic Risks that are rated Extreme or High
- Operational risks that are rated Extreme or High. Risks that are rated Moderate that exceed risk appetite once defined

The CEO may make exceptions to this prioritisation where there is an immediate or foreseeable risk to the health or safety of any person.

Risk treatment options

Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. Options for negative risks may include:

Eliminate	Remove an asset or discontinue an activity or service completely so as to eliminate the risk altogether
Share	Allocate risk to a third party, such as through appropriate contactor management, (noting however that S272 of the WHS Act voids any agreement or contract that purports to transfer any duty owed under the Act.)
Mitigate	Implement a type of treatment control to reduce or remove the risk. This may include but is not limited to options such as substitution (swapping), isolation (barricade), engineering (modify by design) or administration (policy/process)
Accept	<p>Risk can be accepted for a number of reasons including:</p> <ul style="list-style-type: none">– no extra treatments being available;– meets the stated target risk appetite for the type of risk;– informed decision has been made about that risk; and– the cost of risk treatment significantly outweighs the potential risk exposure.

For positive risks, options may include:

Exploit	Implement strategies to capitalise on the likelihood of the risk eventuating and ensure that the organisation is able to respond quickly to the opportunities as they arise
Share	Partnering with another organisation that is able to add skills or value not currently available within Alexandrina Council
Enhance	Influence the factors that will improve the likelihood of the opportunity arising
Accept	Maintain status quo by informed decision

In selecting any risk treatment, consideration must be given to new risks that may arise from implementing it and the processes outlined in this framework applied to those new risks.

Control characteristics

Risk treatments need to be designed in a manner to ensure they are sufficient to mitigate that risk, and have some of the following characteristics if they are to become an adequate control:

- Documented (e.g. policies, procedures, task lists, checklists)
- Systems-oriented (e.g. integrated and/or automated)

- Preventative (e.g. system controls) or detective
- Consistent and regular (including during staff absence)
- Performed by competent and trained individuals
- Clear responsibility and accountability
- Create value (i.e. benefits outweigh costs)
- Achievable for the organisation (based on available resources)
- Evidenced (i.e. documented or electronic audit trail)

Preparing and implementing risk treatment plans

Risk treatment plans specify how the risk treatment options will be implemented, so that those involved understand what arrangements are in place and to allow progress against the plan to be monitored. Risk treatment plans are documented within the (risk register) and project management plans and provide the following information:

- Rationale for selection of treatment options;
- Responsibilities and accountability for approving and implementing the plan;
- Proposed actions and timeframes;
- Resourcing requirements;
- Constraints and contingencies; and
- Required reporting and monitoring.

Monitoring and Review

Review of risks and controls

Monitoring and review involves regular checking or surveillance of the effectiveness and efficiency of the risk management processes implemented.

A monitoring and review process will:

- Ensure that implemented controls are effective and adequate; Provide further information to improve risk assessment and treatment plans;
- Allow for the identification of emerging risks;
- Identify any new factors that may influence established strategies to mitigate risks.

It is essential to monitor all activities and processes in order to capture new or emerging risks arising from the changing environment, (both internal and external) and the activities undertaken by Alexandrina Council's employees, contractors and volunteers.

Monitoring and review guidelines and timeframes are captured in the Risk Reporting structure.

Project risks

Due to the dynamic nature of most projects, a risk may change over the project lifecycle, triggering the need for reassessment. The monitoring and scheduled review process allows for both validation of risks to ensure that they remain relevant and adaptation of project plans as necessary. Any changes in risks throughout the project and following completion should be recorded and used for future project planning.

Internal audit

The internal audit process plays an important role in evaluating the internal controls (and risk management processes) currently employed by Alexandrina Council. The internal audit program is 'risk based' and provides assurance that Council is managing risks appropriately. In developing the Internal Audit Plan, consideration is given to the extreme, high and moderate risks identified by the risk assessment process. Internal audits assess the adequacy of selected controls identified.

The internal audit process will measure risk by:

- a. **Measuring compliance** – has the organisation met its Policy objectives
- b. **Measuring maturity** – measuring against best practice and sector benchmarking
- c. **Measuring value add** – has the framework and risk culture added to the achievement of Alexandrina Council's strategic objectives

Information is shared between the risk management and internal audit functions. Changes in Councils risk profile are reflected in the Internal Audit Plan. The internal audits are conducted to provide assurance that key risks have been identified and the controls in place are adequate and effective, as per the following table.

Rating	Definition
Design adequacy	
Adequate	The control is designed in a manner that it can give reasonable assurance that the risk will be mitigated. In other words, existing systems and procedures cover known circumstances and provide reasonable assurance for majority of risks.
Partially adequate	The control is designed in a way that will partially mitigate the risk and designed in a way to partially meet the design objectives.
Inadequate	The design of the control is not sufficient enough to give reasonable assurance that the risk will be mitigated. There may be no systems and procedures in place, or existing systems and procedures are obsolete and require review.
Operating effectiveness	
Effective	The control operates in a manner that is effective in terms of being consistent, complete, reliable and timely.
Partially effective	The control partially operates in a manner that is effective in terms of being consistent, complete, reliable and timely.
Ineffective	The control does not operate in a manner that is effective in terms of being consistent, complete, reliable and timely.

It is to be noted that the overall combination of the results of design adequacy and operating effectiveness will provide the overall rating of the control based on the table for overall rating. This assists in identifying improvements to existing controls.

	Effective	Partially effective	Ineffective
Adequate	Effective	Partially Effective	Ineffective
Partially adequate	Partially Effective	Partially Effective	Ineffective
Inadequate	Ineffective	Ineffective	Ineffective

Recording and reporting

General

The risk management process and its outcomes will be documented and reported, in order to:

- Communicate risk management activities and outcomes;
- Provide information for decision making;
- Provide opportunities for continuous improvement;
- Assist interaction with stakeholders, including those with responsibility and accountability for risk management activities.

Records will be managed and retained in accordance with State Records General Disposal Schedule for Local Government.

Risk register

The risk register enables the organisation to document, manage, monitor and review strategic, operational and project risk information in order to build a risk profile and provide direction on how to improve risk management processes. The risk register can be used to monitor whether, using the approach outlined in this framework, the risk management process is resulting in an increasing trend towards potential for success and less risk with negative consequences.

Strategic risks

Strategic level risks are identified by the Executive and the Council as part of an annual review at a minimum and will be recorded in the risk register.

Operational risks

Operational risks will be recorded in the risk register, and be reviewed at least bi-annually by Department Managers. Recording operational risks in the risk register and reporting of implementation and effectiveness of controls is the responsibility of department managers and workers.

Project risks

Project level risks may be identified by the project management team at any time prior to, and during, the project management cycle and are initially recorded in the project

management plan and consolidated in the operational risk register. Recording and reporting of project risks rest with the project owner.

Other Reporting

The Internal Audit Group monitors and reviews the adequacy and effectiveness of risk management to provide oversight of the internal control and risk approach via internal and external reports.

At each of its regular meetings, the Internal Audit Group will also consider the Risk Action Plan, significant business incidents or breaches, audit and other independent assurance activity.

This is achieved through:

- Assessing the current state of risk management activity against the Risk Action Plan
- Determining if the current level of risk taken is acceptable (*including current risks which may remain high or extreme where all controls are successfully implemented*)
- Providing advice and expertise on key risk areas and control improvements.

A full review and update of the Strategic Risk Profile will occur as part of each Strategic Planning process (which generally occurs every 2-3 years). Subsequent to this process, in line with the four regular meetings of the Internal Audit Group, the following reporting (and specific agenda items) will occur:

Quarter	Key Risk Management Agenda item
4	<ul style="list-style-type: none">• Strategic Risk Register – entire document (including progress of related planned treatments for these risks) endorsed by the Executive, and tabled at Internal Audit Group, including any new and emerging strategic risks.
4	<ul style="list-style-type: none">• Risk Action Plan (short report format)
4	<ul style="list-style-type: none">• Operational Risks :<ul style="list-style-type: none">➢ Extreme or High Operational risks (post treatment)➢ Presentations by Senior Management on specific Operational Risk Profiles of interest to the Internal Audit Group on a rolling basis to cover complete business operations over a 3-year period

Training

Workers

The risk management policy and framework, together with supporting tools will be made available to all workers through (the intranet) and hard copies provided on all staff notice boards. Risk Management awareness training will be provided to workers and will take into consideration the worker's role and level of past risk management experience and knowledge.

Council Members

Council members are key strategic decision makers and it is therefore imperative that they have an understanding of Alexandrina Council's Risk Management Policy and Framework

and their role in informed planning and decision making. Risk management awareness training will be scheduled within 12 months of Local Government elections.

Internal Audit Group

Internal Audit Group members should, at a minimum, have an understanding of their roles and responsibilities as outlined in Alexandrina Council's Risk Management Policy and Framework, including the monitoring and review of reports and outcomes from management reviews and external audits.

Review of Risk Management Framework

This risk management framework and processes will be scheduled for review within 4 years from endorsement.

Definitions

Assurance	A process that provides a level of confidence that objectives will be achieved within an acceptable level of risk
Consequence	The outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.
Control	An action that modifies risks and increases the likelihood that objectives and goals of an organisation will be achieved.
Corporate Risk Management	The process that is applied in strategy setting and decision making throughout the organisation to identify, evaluate and manage potential risks that are likely to impact on achievement of objectives, set risk appetite and tolerance and manage risk within those parameters, and to provide reasonable assurance regarding the achievement of the organisation's objectives.
Event	Occurrence of a particular set of circumstances
Exposure/Rating	The risk exposure (also referred to as risk rating) is a qualitative value of the sum of the consequence of an event multiplied by the likelihood of that event occurring
External Context	External environment in which the organisation seeks to achieve its objectives
Frequency	A measure of the rate of occurrence of an event expressed as the number of occurrences of their event in a given time.
Internal Audit	An independent, objective assurance activity that uses a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.

Internal Context	Internal environment in which the organisation seeks to achieve its objectives
Likelihood	Chance of something happening
Monitor	To check, supervise, observe critically or record the progress of an activity, action or system on a regular basis in order to identify change.
Reasonable assurance	The concept that enterprise risk management, no matter how well designed and operated, cannot guarantee that an entity's objectives will be met. This is because of inherent limitations in all Risk Management Frameworks.
Risk Analysis	A systematic use of available information to determine how often specified events may occur and the magnitude of their consequences.
Risk Appetite	Is the amount of risk an organisation is prepared to accept in pursuit of its objectives
Risk Assessment	An overall process of risk identification, risk analysis and risk evaluation
Risk Culture	Risk culture refers to the behaviours that lead to how every person thinks about and manages risks,
Risk Evaluation	The process used to determine risk management priorities by comparing the level of risk against predetermined standards, target risk levels or other criteria.
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 Owner	Staff member with the accountability and authority to manage a risk
Risk Tolerance	The acceptable variation in outcomes related to specific performance measures linked to objectives the organisation seeks to achieve
Risk	The effect of uncertainty on objectives
Stakeholder	Person or organisation that can affect, be affected by, or perceive themselves to be affected by, a decision or activity

Appendices

Appendix A: Consequence Tables

Qualitative Measures of Consequence (excluding Project Risks)

Rank	People	Financial/ Infrastructure	Service Delivery	Reputation	Environmental/ Cultural site disturbance	Legal/ Regulatory/ Policy
Insignificant	No or minor injuries not requiring first aid treatment, or near miss Annual staff turnover of <10%	Financial – low financial loss <\$100,000 impact on operating result Minor failure of infrastructure – no inconvenience to stakeholders	Insignificant interruption to a service – no impact to customers/ business	Little community interest, low profile, no media items	Minor instance of environmental (e.g. soil, vegetation, coastal) damage. can be reversed immediately Minimal (but discernible) disruption to Aboriginal site. Minimal spill or litter able to be removed immediately	No noticeable statutory or regulatory impact Fines < \$10,000
Minor	First aid treatment. Negligible impact on morale Annual staff turnover of <20%	Financial – medium financial loss >\$100,000 and <\$1,000,000 or 1% of rate revenue Minor failure that cannot be rectified immediately – minor inconvenience to stakeholders	Minor interruption to a service with minimal impact to customers/ business	Low impact, some passing interest, low media profile	Minor impact to environment, e.g. on-site chemical release, spill or sand/soil movement that can be immediately contained. Can be reversed in the short term Minor disruption to Aboriginal site Litter able to be removed in a short time frame, (e.g. same day)	Minor/temporary non-compliance with statutory requirements Fines less than \$250,000 for the organisation

Rank	People	Financial/ Infrastructure	Service Delivery	Reputation	Environmental/ Cultural site disturbance	Legal/ Regulatory/ Policy
Moderate	<p>Medical attention required. Short Term effect on morale and business</p> <p>Annual staff turnover of >20% of entire workforce or 30% of a work group</p> <p>Loss of member of Executive Management Team</p> <p>Loss of up to 4 (Council/Board) members more than 12 months out from LG Elections [drafting note: this number would be the total number of members minus number required for quorum]</p>	<p>Financial – high financial loss >\$1,000,000 and <\$2,500,000 or 2.5% of rate revenue</p> <p>Significant failure of infrastructure that will require work-arounds - moderate inconvenience to stakeholders</p>	<p>Moderate Interruption to service delivery. Customer impact up to 48 hrs. Partial BCP action may be needed</p>	<p>Moderate impact, moderate public interest, public embarrassm ent, moderate media profile</p>	<p>Moderate impact to environment. Localised damage or chemical release that has potential to spread but can be contained or reversed with intensive efforts or outside assistance</p> <p>Noticeable disruption to Aboriginal site</p> <p>Litter removal requires outside assistance, (e.g. contractor or government agency)</p>	<p>Short-term non-compliance with moderate statutory requirements</p> <p>Fines < \$50,000 for an individual or < \$500,000 for the organisation</p>

Rank	People	Financial/ Infrastructure	Service Delivery	Reputation	Environmental/ Cultural site disturbance	Legal/ Regulatory/ Policy
Major	<p>Extensive injuries - serious long term injury. Temporary disablement.</p> <p>Annual staff turnover of 30% - <75%</p> <p>Significant impact on morale and business</p> <p>Loss of 2 members of Executive Management Team</p> <p>Temporary loss of 6 or more (Council/Board) Members <i>[drafting note: this should be the number that will prevent a quorum being formed]</i></p>	<p>Financial – major financial loss >\$2,500,000 and <\$5,000,000 or 5% of rate revenue</p> <p>Major failure of infrastructure that severely limits functionality – significant inconvenience to stakeholders</p>	<p>Major interruption to service delivery or production capability, Customer impact > 7 days. Component of BCP action may be needed.</p>	<p>Sustained public interest, high negative media profile, Premier/Cabi net publicly involved, third party action</p>	<p>Off-site chemical release, severe loss of environmental amenity or danger of continuing environmental damage.</p> <p>Significant disruption to Aboriginal site(s)</p>	<p>Significant non-compliance with essential statutory requirements</p> <p>Fines <\$300,000 for an individual or < \$1,500,000 for the organisation</p>

Rank	People	Financial/ Infrastructure	Service Delivery	Reputation	Environmental/ Cultural site disturbance	Legal/ Regulatory/ Policy
Catastrophic	<p>Death.</p> <p>Long term effect on morale and performance of business</p> <p>Annual staff turnover of > 75%</p> <p>Loss of entire/majority of Executive Management Team</p> <p>Permanent loss of 6 or more Council Members</p>	<p>Financial – huge/ catastrophic financial loss/exposure >\$5,000,000 or 5% of rate revenue</p> <p>Total failure of infrastructure</p>	<p>Major interruption to delivery of all or most services for more than 14 days. Full BCP action required.</p>	<p>Widespread public agitation, Government censure, high multiple impacts, widespread negative media profile</p>	<p>Toxic off-site chemical release with detrimental effect, major loss of environmental amenity or irrecoverable environmental damage</p> <p>Irreversible disruption to Aboriginal site</p>	<p>Long term or indefinite non-compliance with essential statutory requirements and may result in criminal charges</p> <p>Fines > \$300,000 for an individual or > \$1,500,000 for the organisation</p>

Consequence Table for Project Risks

Rank	Cost	Schedule	Performance	Reputation	Safety
Insignificant	< 2.5% of total Project Budget	< 2.5% of total Project Schedule	Would cause the delivered capability to be functionally fit for all desired missions or tasks, but there may be some qualification to the level to which it would perform non-critical elements of the mission or task. Few such qualifications would exist.	Little community interest, low profile, no media items	Minor injuries not requiring first aid treatment, or near miss
Minor	2.5-10% of total Project Budget	2.5-10% of total Project Schedule	Would cause the delivered capability to be functionally fit for all desired missions or tasks, but there would be some qualification to the level to which it would perform non-critical elements of the mission or task. Several such qualifications would exist.	Low impact, some passing interest, low media profile	Minor Medical attention. Negligible impact on morale

Rank	Cost	Schedule	Performance	Reputation	Safety
Moderate	10-14% of total Project Budget	10-14% of total Project Schedule	Would cause the delivered capability to be partly functionally fit for purpose (i.e. degraded ability to perform all desired missions or tasks; however, there are known workarounds). There would be some qualification to the level to which it would perform (e.g. due to issues of relationships, concurrency, etc.). Several such qualifications would exist.	Moderate impact, moderate public interest, public embarrassment, moderate media profile	Medical attention required. Short Term effect on morale and project outcome.
Major	15-19% of total Project Budget	15-19% of total Project Schedule	Would cause the delivered capability to be only partly functionally fit for purpose (i.e. degraded ability to perform some core missions or essential tasks or unable to perform non-core missions or tasks, and there are no known workarounds).	Sustained public interest, high negative media profile, Premier/Cabinet publicly involved, third party action	Serious Long Term Injury. Temporary disablement. Significant impact on morale and project outcome.
Catastrophic	>20% of total Project Budget	>20% of total Project Schedule	Would cause the delivered capability to be functionally unfit for its intended purpose (i.e. unable to perform core missions or essential tasks).	Widespread public agitation, Government censure, high multiple impacts, widespread negative media profile	Death. Long term effect on morale and project outcome.

Appendix B: Likelihood Table

Likelihood	Explanation – Operations	Explanation – Projects/ Business Case	Probability
Certain to occur	It is expected to occur in most circumstances, immediately or within a short period – at least once a year	Could be expected to occur more than once during the study or project delivery	Expected to occur in most circumstances
Very likely	Will probably occur in most circumstances – Around 1 – 5 years	Could easily be incurred and has generally occurred in similar studies or projects.	Probably will occur
Possible	Might occur at some time - within a 5 - 10 year period.	Incurred in a minority of similar studies or projects	Moderate probability of an incident
Unlikely	Could occur at some time - in a 10 – 20 year time frame.	Known to happen, but only rarely.	Low probability of an incident
Rare	May occur only in exceptional circumstances. Could be incurred in a greater than 20 year timeframe.	Has not occurred in similar studies or projects. Conceivable but in extreme circumstances.	Extremely low probability. Will only occur in exceptional circumstances

Appendix C: Risk Matrix

Consequence Likelihood	Insignificant	Minor	Moderate	Major	Catastrophic
Certain to occur	High	High	Extreme	Extreme	Extreme
Very likely	Medium	High	High	Extreme	Extreme
Possible	Low	Medium	High	Extreme	Extreme
Unlikely	Low	Low	Medium	High	Extreme
Rare	Low	Low	Medium	High	High