Strathbogie Shire Council Risk Management Policy

October 2022

Strathbogie SHIRE COUNCIL

Contents

Risk Management Policy

Document ID:	12147
Effective Date:	September 2013
Last Review:	June 2019
Current Review:	October 2022
Date Adopted by Council:	18 October 2022
Next Scheduled Review Date:	October 2023
Responsible Officer:	Director People and Governance

PART 1 POLICY

1. PURPOSE

Through integration with the approved Risk Management Framework, the purpose of this policy is to:

1. Establish the principles upon which our organisational risks are managed in accordance with the risk management standard, ISO 31000:2018 Risk Management – Guidelines.
2. Guide the integration of risk management driving continuous improvement into our organisational culture, daily business practices and strategic planning processes.
3. Implement an approach to risk management that is fit for purpose at all levels throughout Council.
4. Integrate risk based decision-making across the elected Council and organisation for the benefit our community and stakeholders.
5. Develop a culture of risk awareness, accountability and shared attitudes that promotes a willingness and capability to manage risk at all levels across the organisation and elected Council.
6. Create an effective risk management framework so that all staff understand the business risks in their area and actively manage those risks as part of their day-to-day activities.
7. Clearly identify roles and responsibilities in creating and maintaining a robust risk management framework.

2. POLICY STATEMENT

This policy is a core component of Council's corporate policy framework and Risk Management Framework. Through this policy and associated documents, Council's approach to risk management will be:

1. Proportionate to the size of the organisation, recognising the limitations on the resources of a small rural shire, targeting effort and resources to the areas of highest priority.

2. Integrated into all our activities and functions, therefore forming an integral part of all that we do and the way we deliver services.

3. Agile, forward thinking and flexible in its design and application so that quick responses can be made to unexpected changes and events outside of Council's control.

4. Focused on continuous learning and improvement.

5. Compliant with our legislated obligations

6. Adding value through each step of the risk management process.

7. Efficient to operate and maintain, avoiding administrative burden wherever possible.

Council accepts that, on occasions, even with sound risk management practices, things may go wrong. On such occasions, we will take the opportunity to review the reasons for the failure and endeavour to further strengthen controls to reduce the likelihood of a reoccurrence.

3. APPLICATION OF THIS POLICY

This policy applies to all areas of Council operations and is to be understood and implemented by all Councillors, staff, contractors and volunteers undertaking any function for or on behalf of Council.

4. ACCOUNTABILITY AND RESPONSIBILITIES

Role	Responsibilities
Elected Council	The overall responsible body for the review and adoption of this policy and the Enterprise Risk Management Framework. Accountable for risk management at Council. Set the risk appetite and has a role is identifying, assessing and managing strategic risk. Receives advice and recommendations from the Audit and Risk Committee.
Audit and Risk Committee	Independent review and oversight of Council's risk management framework and control activities, with a focus on monitoring the Strategic Risk Register. Management and oversight of the internal audit function. Oversight of Council's compliance with legislation and Council policies and procedures. Programs the internal audit calendar.

Internal Auditors	Provide risk based internal audits to the Audit and Risk Committee based on the internal audit calendar, identifying management actions and risk controls to address identified risks to drive continuous improvement.
Chief Executive Officer	Overall accountability for risk management. Promote risk management as a vital business principle, provide a safe and healthy work environment and enable employees to meet their duty of care to in protecting its people, community, assets and operations. Set the tone, culture and expectations for risk management and governance activities. Ensure adequacy of resources for risk management activities. Set appropriate delegations of Risk Management Functions.
Executive Leadership Team	Implement the risk management framework, ensuring appropriate resources for risk management actions are made available and ensuring effective monitoring, reviews and reporting are undertaken. Promote risk management as a vital business principle, monitor and evaluate the performance of managers against their risk management accountabilities and assist managers in the identification, evaluation and mitigation of risks. Own and manage risks in their respective portfolios. Ensure staff performance in compliance with and implementation of this policy and the Enterprise Risk Management Framework. Update the Strategic Risk Register and ensuring operational risk registers for their areas are in place and updated. Drive a positive and proactive risk management culture based on continuous improvement in our service delivery.
Director People and Governance	Oversight of implementation of this policy and its procedures, leading the risk management function. Development of a risk management framework that is fit for purpose. Responsible for Audit and Risk Committee agendas and minutes. Responsible for ensuring updates to the Strategic Risk Register are reported to the Audit and Risk Committee. Responsible for ensuring training and support is provided to the organisation, elected Council and Audit and Risk Committee around the implementation of this policy and the achievement of a proactive risk management culture.
Corporate Risk Officer	Risk reporting to the CEO and Audit and Risk Committee. Develop and deliver a risk management training program. Monitor organisational compliance with implementation, review and maintenance of risk management procedural requirements. Support for the organisation to manage its risks through: • Assisting employees with the procedural aspects of risk management • provision of risk management advice and guidance • maintenance of the risk management framework.

Managers	Understand the principles of risk management. Proactively manage risks and monitoring control effectiveness in accordance with Council's approved risk management framework. Ensure compliance by staff with this policy at all times. Ensure risk management analyses and plans are in place for core functions and responsibilities. Updates of the Strategic Risk Register and operational risk registers for functions under their portfolios. Assist Direct reports in the identification, evaluation and mitigation of risks associated with their day to day functions. Enter all risks within their jurisdiction onto the Risk Register. Keep employees appropriately informed of all changes relating to registered risks. Advise of any risk issues within their jurisdiction that should be incorporated in forthcoming budgets. Foster and cultivate an appropriate risk management culture across the organisation.
All Staff, Volunteers and Contractors	Applying sound risk management practices in accordance with Council policies and frameworks. Adopting a proactive risk management culture at all times in their day-to-day operations. Assist their manager in the identification and management of risks to be entered into the risk register. Contribute to the development and implementation of risk treatment plans and strategies within their work area. Provide timely assistance and requested information in relation to any insurance claim or risk management issue. Make loss control/prevention a priority whilst undertaking daily tasks. Complete a formal risk assessment for proposed events and projects. Perform their duties in a manner that does not represent an unacceptable level of risk to the health and safety of themselves, other employees, the customers or visitors, contractors or the wider community. Report any illness, injury, hazard, near miss or incidents and losses as soon as they are detected to their manager or supervisor.
Contract/Tender Managers	Ensure that tenders issued, and contracts let, comply with the risk management, insurance and indemnity requirements of Australian Standard AS 4000/1997 General Conditions of Contract and conform to the intent of the Risk Management Policy and Framework.

5. ENTERPRISE RISK PROFILE STRUCTURE

There are three levels of risk:

Level 1 Strategic and organisational risks

Strategic risks are forward looking and linked to the strategic objectives. The time horizon for these risks are typically the time horizon of the strategic plan (i.e. four-years) Strategic risks are few and externally focused. Organisational risks are linked to the strategic risk and are the risks that impede the delivery of strategic objectives.

A control not well designed or managed may be the source of a risk.

Organisational risks are internally focused and identify the critical controls required to enable the delivery of the Council Plan.

Level 2 Operational risks

Operation risks are the risks focused on delivering business objectives, compliance objectives and are function based. The time horizon for these risks are aligned to service or business plans. Operation risks are linked to strategic risks.

Level 3 Project risks

Project and event risks are risks linked to the delivery of a project and focus on changes to scope, budget, schedule and the project quality.

6. OUR RISK MANAGEMENT APPROACH

Our approach to risk management involves the following four steps:

Throughout this process, communication and consultation with relevant stakeholders, staff and where appropriate the Audit and Risk Committee and Council, will be key to ensuring a comprehensive approach to managing and mitigating risk.

Risk assessments and managements must be living documents and at all times we will:

Plan: Plan what departments and services should do to work safely informed reviews of the strategic register and operational risk assessments.

Implement: Put into practice the control measures to minimise the risk across the organisation. Controls can be in many forms including policies, procedures, technology, reporting or skill development/training.

Monitor: Keep checking to see how well the control measures are working.

Improve: Address any issues and find ways to make what the business is doing even more effective.

7. RISK ANALYSIS AND ESCALATION CRITERIA

The purpose of risk analysis is to comprehend the nature of risk and its characteristics including where appropriate, the level of risk.

The main objective of risk analysis is to separate the minor acceptable risks from the major ones and to provide data to assist in the evaluation and treatment of risk.

Risk analysis involves a detailed consideration of risk uncertainties, risk sources, consequence, likelihood, event, scenarios, controls and their effectiveness.

When determining the likelihood or consequence of a risk occurring, it is important to take into consideration existing controls.

7.1 Risk rating

A risk analysis will result in overall risk rating.

A full, accurate and objective assessment of any identified risk must be undertaken to:

- evaluate the effectiveness of existing controls
- determine the consequences of the risk
- determine the likelihood of consequences occurring as a result of a specific risk
- determine the level of risk to judge its importance or acceptance to the organisation
- prioritise risk based on their assessed level and the organisation's tolerance of the risk
- identify remedial actions allocate appropriate resources for its treatment.

There are two main factors applied when analysing risks – consequences and likelihood.

1. Determining consequences

The consequence of a risk can usually be expressed as a measure of financial loss, impact upon achieving business or project initiatives, reputational damage or safety impacts.

Consequences are usually determined on the basis of "most credible worst case scenario" recognising that "worst case scenario" is not usually what is experienced.

The estimation of consequence needs to be done in full consideration of the effectiveness of the risk controls already in place. Criteria for assessing the consequences of a risk are summarised in Table 1.

Table 1 Determining Risk Consequences

Parameter	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Safety	Medical treatment injury Temporary, minor health impact on staff or public	Multiple medical treatments or lost time	Serious health impact on member of the public - more than 10 days rehabilitation required for injured staff member	Loss of key member of management team - serious health impact on multiple members of staff or public	Multiple or single fatalities - public or staff. Loss of a significant number of employees
Parameter	**Insignificant** **1**	**Minor** **2**	**Moderate** **3**	**Major** **4**	**Catastrophic** **5**

Revenue, Cost or Liability	Cost to Council - < $50,000	Cost to Council - $50,000 to $200,000	Cost to Council - $200,000 to $2.5M Fines to Council personnel	Cost to Council - $2.5M to $5M Council officer or Councillor convicted	Cost to Council - > $5M Curbing of programs required due to significant shortfall in revenue or blow out in expenditure Intervention by Local Government Minister
Environment	Minor release of pollutants which does not require notification to third parties - brief nonhazardous temporary pollution	Required to inform EPA - Contained temporary pollution	Significant release of pollutants - residual pollution requiring clean-up work	Major release of toxins/water resulting in high compensation or reconstruction costs Likelihood of legal prosecution by EPA	Major release of toxic waste resulting in long term damage to the environment
Probity and Political	Marginal impact on Council operations Minimal to no effect on reputation - Resolved in day-to-day management	Inadequate probity being exercised. Minor/isolated concerns raised by members of public, customers, suppliers	Public/media negative attention Local community concern Customer or supplier concern	Public/media concern Damage to Council's reputation Council subject to formal inquiry/sanction	Public/media outrage Public pressure to curtail operations of Council
Information Systems and Business Interruption	Minor disruption to system with no downtime Negligible impact on service provision	Disruption to system with some downtime Insignificant impact on generation of information Brief service interruption (1 day)	Temporary loss of key data Impact on generation of management information Temporary recoverable service failure Interruption of service (2 days)	Serious disruption to system leads to more than 3days downtime (loss of key data and customer support) Service or provider needs to be replaced	Collapse of major system leading to unrecoverable loss of core data. Service removed or unable to function for over one week

2. Determining Likelihood

The "likelihood" of a risk happening is the likelihood of an event occurring with a particular consequence as determined above. An estimation of likelihood is based on a consideration of the effectiveness of the controls known to be in place. As with determining consequence, it is the likelihood of an event occurring with the predetermined "most credible worst case scenario.

The following table outlines how, in the current control environment, the likelihood that a risk will occur is to be estimated.

Table 2 Evaluating Likelihood

Likelihood	Recurrent Risks	Single Event
1. Rare	Only occur as a "100 year event"	May only occur in exceptional circumstances – probability very small, close to zero
2. Unlikely	Could occur in "years to decades"	May occur but not anticipated – probability low but noticeably greater than zero
3. Possible	Could occur within "months to years"	Might occur at some time – less than 50% chance but still quite high
4. Likely	Could occur within "weeks to months" or may arise about once per year	Will probably occur in most circumstances – at least 50/50 chance or greater
5. Almost Certain	Risk is occurring now, or could occur within "days to weeks", or could occur several times per year	Is expected to occur in most circumstances – probability high (e.g. greater than 90%)

Calculating the Overall Risk Rating

Evaluating risks involves determining what risks can be tolerated and those that cannot.

The overall risk rating (RR) is a product of the likelihood (L) multiplied by the severity/consequence (S) of the risk as outlined in Table 3.

Table 3 **Overall Risk Rating Matrix**

Identifying Risk Ratings								
Risk rating guidance	Likelihood (L)	Almost Certain 5	5 Low	10 Medium	15 High	20 Extreme	25 Extreme	Likelihood (L) x Severity (S) = Risk rating (RR).
		Likely 4	4 Low	8 Medium	12 High	16 Extreme	20 Extreme	
		Possible 3	3 Low	6 Low	9 Medium	12 High	15 High	
		Unlikely 2	2 Low	4 Low	6 Low	8 Medium	10 Medium	
		Rare 1	1 Low	2 Low	3 Low	4 Low	5 Low	
			Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5	
			Severity/Consequence (S)					

7.2 Risk Appetite

The risk appetite is the amount and type of risk that an organisation is willing to take in order to meet its strategic objectives. It is best described as an organisation's pursuit of risk or its willingness to take risks rather than avoiding them. This is because it is extremely difficult to introduce control measures to eliminate risks altogether.

The Enterprise Risk Management Framework provides guidance on our risk appetite through stating that Council will take measured risk, informed by a robust risk management framework to inform decision making.

The table below identifies the definitions for our risk appetite and the levels of intervention required for each.

Table 4 Risk Tolerance and Intervention levels

Extreme risk: 16 - 25	Extreme risks are far outside tolerance levels. Activities should cease immediately if at all possible. Extreme risks are to be escalated immediately to the Executive Leadership Team (ELT). Further effective control measures to mitigate risks must be introduced to reduce the risk as a matter of urgency – within 1 week and with ongoing ELT oversight.
High risk: 12 - 15	Risk is outside of tolerance levels. Escalate promptly to the relevant member of the Management Group. Requires prompt treatment to commence within 2 weeks, with ongoing oversight from the relevant Management Group representative(s) and Corporate Risk Management Officer.
Medium risk: 6 - 11	Risk is on the tolerance boundary. Escalate to management. Treatment plan to commence within 8 weeks with regular oversight from the Management Group and Corporate Risk Management Officer.
Low risk: 1 - 6	Risk is within tolerance boundaries but outside of the preferred operating range. Treatment options and oversight plan to be developed with the Management Group.

7.3 Risk treatment

Once the overall risk rating and the intervention level have been identified, attention then moves to risk treatment options.

Strategic risks are managed through the Strategic Risk Register, which is reviewed by the Executive Leadership Team and the Audit and Risk Committee on a quarterly basis, and then submitted to Council for review and consideration.

The Operational Risk Register and the risk profile are managed by the Corporate Risk Officer, supported by the Elumina system which records and monitors treatment activities. The key elements of this system are recording:

- **Risk** – What could happen and how serious could it be?
- **Causes** – Why/how could the risk event happen?
- **Controls in place** - What is in place to mitigate/manage the risk?

- **Control effectiveness rating** – When was the control last reviewed and how effective was it at managing the risk?
- **Current risk rating** – Given the effectiveness of risk controls, how significant is the risk now?
- **Treatment** - What more needs to be done to manage the risk? Depending on the materiality of the current risk exposure, there are several risk treatment options available.

In summary, risk treatment options, as defined by the Enterprise Risk Management Framework, are:

Table 5 Risk treatment options

Decision	Indicators
Remove/avoid the risk	Removing the risk by not proceeding with the policy, program or activity or choose an alternate means of action.
Retain/accept the risk	Council has made an informed decision not to treat the risk, because: a) The cost of controlling outweighs the benefits from controlling the risk, or b) There are no effective controls available to reduce or eliminate the risk. Where any risk ranked low or above are accepted, justification of acceptance is required and a record included in the risk register system.
Treat the risk	Decide to apply controls or other mitigating activities designed to reduce the likelihood and/or consequences of the risk event occurring.
Transfer/share the risk	Share the responsibility with another party such as an insurer/contractor who shares the loss if the risk event were to occur.
Increase the risk	Consciously taking on risk to pursue an opportunity and achieve desired outcomes of a strategy, project or initiative.

8. DEFINITIONS

Term	Meaning
Audit And Risk Committee	means the committee appointed by Council under section 53 of the *Local Government Act 2020*
Audit And Risk Committee Charter	means the charter adopted by Council to outline the composition, roles and responsibilities of the Audit and Risk Committee.
Control	means a measure that maintains or modifies risk. It can take many forms, for example a control maybe policies and procedures (providing instruction), technology (systems), reporting, or people (capability) controls that reduce the consequence and or rectify a failure after it has been discovered, such as continuous improvement actions, crisis

	management, business continuity and or disaster recovery plans and insurance.
Council	means the Strathbogie Shire Council
Enterprise Risk Management Framework	means the set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation. It includes procedures for the day to day implementation of risk management.
Executive Leadership Team	means the direct reports to the Chief Executive Officer
Level Of Risk	means the magnitude of a risk or combination of risks expressed in terms of the combination of severity/consequences and their likelihood of occurring.
Likelihood	means the chances of something happening.
Severity/Consequence	means the outcome of an event affecting Council objectives – it can be certain or uncertain and have either a positive or negative direct or indirect affect.
Management Group	means the group comprised of managers and coordinators
Monitoring	means continual checking; supervising, critically observing or determining the status to identify change from the performance level required or expected.
Operational Risk	means a risk which occurs in or hampers or effects an individual team or function within Council in achieving its plans
Residual Risk Rating (RRR)	means the risk remaining after risk management treatments and controls have been applied.
Risk	means how uncertain future events could influence the achievement of Council's strategic and operational objectives.
Risk Analysis	means the process to comprehend the nature of the risk and to determine the level of risk.
Risk Appetite	means the amount and type of risk that an organisation is willing to take in order to meet its strategic objectives. It is best described as an organisation's pursuit of risk or its willingness to take risks rather than avoiding them.
Risk Management	means coordinated activities to direct and control an organisation in relation to risk.
Risk Management Plan	means the scheme within the risk management Framework specifying the approach, components and resources to be applied to the management of risk
Risk Owner	means the person or entity with the accountability and authority to manage a risk and implement controls to mitigate the risk.
Risk Tolerance	means the level of risk that Council is prepared to accept before action is considered necessary to reduce it and represents a balance between the potential benefits of a calculated risk and the threats that inevitably brings
Strategic Risk	means a risk that will effect or hamper the organisation in its ability to operate or deliver its services.

9. RELATED POLICIES AND LEGISLATION

Local Government Act 2020
ISO 31000:2018 Risk Management – Guidelines
Enterprise Risk Management Framework
Council Plan 2021-25
Audit and Risk Committee Charter

10. POLICY REVIEW

Council may review this policy at any time and at least two years from the date of adoption or the completion of the last review.

Minor amendments to the policy may be authorised by the CEO at any time where such changes do not alter the substance of the policy (e.g. a change to the name of a related document, or a change in legislation).

11. CHARTER OF HUMAN RIGHTS AND RESPONSIBILITIES ACT 2006 AND THE EQUAL OPPORTUNITY ACT 2010

The Council acknowledges the legal responsibility to comply with the *Charter of Human Rights and Responsibilities Act 2006* and the *Equal Opportunity Act 2010*. The *Charter of Human Rights and Responsibilities Act 2006* is designed to protect the fundamental rights and freedoms of citizens. The Charter gives legal protection to 20 fundamental human rights under four key values.