Strathbogie Shire Council

Risk Management Framework

June 2024

Strathbogie
SHIRE COUNCIL

Contents

Risk Management Framework

Document ID:	369691
Effective Date:	18 June 2019
Last Review:	June 2019
Current Review:	May 2024
Date Adopted by Council:	18 June 2024
Next Scheduled Review Date:	February 2026
Responsible Officer:	Director People and Governance

1. OVERVIEW

The *Strathbogie Shire Council Plan 2021-2025* (the Council Plan) outlines the five-year strategies that will help Council to achieve its goals and building flourishing communities in the Shire.

The Risk Management Framework is a key component of Council's governance arrangements and is the structure upon which the risks, opportunities and other information that may impact upon the achievement of Council's goals and strategies to be identified and managed. Through the Risk Management Framework, risk management practices can be applied consistently right across Council which enables Council to confidently make decisions that are timely, informed and cognisant of the factors that may impact upon the success of the Plan.

The Risk Management Framework is based upon the International Risk Management Standard (adopted here in Australia) ISO 31000:2018, (the Standard) which outlines the approach to risk management that is followed in both the public and private sectors in Australia. The Risk Management Framework (the Framework) outlines the arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout Council.

The Framework applies to all operational areas of Council, including Councillors, Council staff, contractors and volunteers undertaking any function for or on behalf of Council.

2. OBJECTIVES FOR COUNCIL'S MANAGEMENT OF RISK

The key purpose for the management of Council's risks is to help Council achieve goals and objectives which are outlined in the Council Plan and the operational plans for each business unit.

Council's approach to risk management is designed to:

- Support the Councillors, Executive and management to confidently make informed decisions based on organisational policy, values and appetite;
- Assist Council to achieve organisational objectives through the systematic and timely identification and management of risks and exploitation of strategic opportunities;
- Consistently manage the effects of uncertainty through the application of robust risk management practices;
- Promote compliance with relevant obligations; and
- Create and protect value by targeting effort and resources to the areas of highest priority.

Application of the Risk Management Framework will assist Council to:

- Achieve its goals and the Council Plan priorities and actions;
- Protect the safety of people, assets, finances and Council reputation;
- Take risks in accordance with approved policies and organisational values;
- Adopt risk treatment activities that are fit for purpose, cost effective and are designed to reduce risk to an acceptable level; and
- Embed a culture that promotes awareness and accountability for risk, so it becomes a normal way that business is done at Council.

3. PRINCIPLES AND COMPONENTS OF THE FRAMEWORK

Council's Risk Management Framework is designed on the following principles:

- Fit for purpose.
- Adds value in each step or activity.
- Is efficient to operate and maintain.
- Avoids administrative burden.
- Promotes integration of risk throughout Council
- Helps the Executive and management to discharge their duties and responsibilities.

The Framework is the totality of all documents, processes, systems and personnel that operate the framework for the purposes of risk management at Council. As detailed in Table 1, the Risk Management Framework comprises:

Table 1: Risk Management Framework Components

Outlined In Separate Documents	Outlined In This Document
• Risk Management Policy	• Risk Management Framework (the Framework)
• Audit and Risk Committee Charter	• Risk governance structure
• Operational and Strategic Risk Registers	• Three lines of defence
	• Risk categories
	• Risk appetite and tolerance statement
	• Risk rating matrix
	• Risk profile
	• Risk register system
	• Risk culture and reporting

Risk Management Procedures

Council's *Risk Management Procedures* document provides detail on the application of the tools outlined in this Risk Management Framework document.

The procedures are based on the risk management standard, ISO 31000:2018 as detailed in Figure 1 below.

Figure 1: Risk process. Source: ISO31000:2018

Risk Management Governance Structure

Council's Risk Governance Structure is a component of the overall organisational structure. It represents the accountability and responsibility for risk, reporting lines for risk information and risk escalation path.

The Risk Governance Structure starts with the Councillors and cascades through management and all levels of staff. Oversight for risk is achieved through the Audit and Risk Committee and management and executive committees, with independent assurance from the internal audit function.

Figure 2: Council Risk Management Governance Structure

Risk Management Function

Council's risk management function is comprised of a Risk Officer. As outlined in the above governance structure and the Risk Officer's position description, the Risk Officer:

- Is responsible for assisting senior management to develop, implement and maintain the Risk Management Framework;
- Has an appropriate level of operational independence as a second line of defence function;
- Has the right capability and capacity that is fit for Council's purposes; and
- Has the necessary access to business units, management and staff to conduct risk management activities and appropriate reporting lines through to the Audit and Risk Committee.

Key responsibilities of the Risk Officer are facilitating regular risk profiling, enterprise risk reporting, maintenance of the Risk Management Framework and risk registers and working with Council divisions to assist and advise on the application of the Risk Management Framework.

4. RESPONSIBILITIES AND ACCOUNTABILITIES

Table 2: Roles, Responsibilities, and Accountabilities for Risk Management

Role	Responsibilities and Accountabilities
Councillors	• Oversight of risk management at Council (including setting the Risk Appetite) • Oversight of the Audit and Risk Committee.
Chief Executive Officer	• Overall accountability for risk. • Setting the tone, culture and expectations for risk management and governance activities. • Ensuring resources for risk management activities are adequate for Council purposes. • Setting appropriate delegations for the risk management function.
Audit and Risk Committee	• Independent review and oversight of Council's adherence to the governance principles in the *Local Government Act 2020*, risk management and control activities. • Oversight of the internal audit function.
Internal Audit	• Risk assurance to the Audit and Risk Committee and CEO through execution of the internal audit plan.
Executive Leadership Team (ELT)	• Accountable for ownership and management of risks in their respective areas of responsibility. • Role modelling the tone, culture and expectations for risk management and governance activities. • Oversight of risk management across Council.

Managers/People Leaders	• Responsible for management of risks in their respective divisions/business units, in accordance with the Risk Management Framework. • Responsible for the risk management performance of staff in their respective divisions/business units.
Risk Officer	• Coordinating the risk management function. • Developing, implementing and maintaining a Risk Management Framework that is fit for purpose. • Risk reporting to the CEO and Audit and Risk Committee. • Supporting the organisation to manage its risks through the provision of risk management advice and guidance to staff.
All Staff And Contractors	• Applying sound risk management practices in accordance with Council policies and frameworks.

5. THREE LINES OF DEFENCE – RISK ASSURANCE

Council operates a 'three lines of defence' (3LOD) model to actively manage, monitor and oversee risk. This model comprises:

First Line of Defence - Operational management, including divisional staff and management

The first line of defence. Management owns the risks attributable to their area of responsibility and are accountable for the appropriate management of risk and the effectiveness of risk controls. It is imperative that management understand and accept their accountability for owning and managing their risks. This accountability cannot be delegated to another function, such as the Risk Officer.

For example, Management in the Finance team are accountable for all risks pertaining to financial management and are the financial risk owners. Divisional Management are also responsible for financial risk in their respective divisions and teams and for applying the organisation's financial risk management policies, frameworks and tools. This is the first line of defence's responsibility. Assurance over the effectiveness of financial controls may be obtained through a *risk and control self-assessment* conducted by divisional management.

Second Line of Defence - Enterprise risk, compliance, legal counsel, IT security

The second line works with management to help design appropriate risk controls, monitor risk treatments and report to senior management. This activity may be conducted at a business unit or divisional level, (e.g., assisting the unit to assess and monitor project risks) or at an organisational level (e.g., assessing and reporting the risks and opportunities in development and implementation of the Council Plan).

In the financial risk example, the role of the second line of defence, the Risk Officer is to assist management to apply the Risk Management Framework to identify and manage financial risks. This may be through ensuring risk profiling workshops occur, advising on the design of

financial risk controls and reporting on financial risks to the executive or other governance committee.

Third line of defence – Internal Audit (IA)

The Internal Audit function is independent of management and hold no operational responsibilities. Internal Auditors primary role is to provide objective and independent assurance to Council, the Audit and Risk Committee and senior management over the effectiveness of internal controls, risk management and governance activities.

Assurance activity is guided by the internal audit plan. It is an efficient use of resources to integrate risk management into the internal audit plan. That is, the internal audit plan takes into consideration Council's risk profile and targets assurance activities towards higher rated risks and/or matters of high priority to management. The internal audit plan avoids duplication where possible and takes into consideration the assurance activities performed by independent parties such as external audit, VAGO, external consultants, or a *risk and control self-assessment* performed by divisional management.

In the financial risk example, it is prudent for Internal Auditors to regularly review an organisation's financial risk controls to assess for appropriate control design and operating effectiveness. The frequency of this review will depend on the current level of financial risk the organisation is managing, the need for independent assurance and the value expected to be obtained from this review.

Table 3: Components of the Three Lines of Defence model at Council

First Line of Defence	Second Line of Defence	Third Line of Defence
All management in the Strathbogie Shire Council Directorates • Innovation and Performance • Community Assets and Infrastructure • Corporate and Community	• Enterprise Risk • Compliance • OHS • IT security	• Internal audit (outsourced providers of internal audit activities) Note that internal audits are separate to the external audit whose role is to review the integrity of Council's financial records.

6. INTEGRATION OF RISK INTO COUNCIL ACTIVITIES

Integrated risk management is an organisation-wide approach to addressing risk that involves input from all teams and centres risk as a fundamental part of business strategy. Council has adopted a set of processes and best practices to improve the performance and decision-making of the organisation through the integrated views of how the organization manages its risks.

Figure 3 below details the integration required for effective risk management.

Figure 3: Risk framework. Source: ISO31000:2018

1 Leadership and Commitment

Accountability for risk is promoted through the Councillors, CEO, Audit and Risk Committee and Executive Leadership Team and endorsed through the Risk Policy and the Risk Management Framework. Further, the risk appetite statement demonstrates Council's commitment and philosophy for risk management.

Council's leaders are measured on their commitment to risk management through their position descriptions. Staff are measured through their application of, and adherence to, the Risk Management Framework.

2 Integration

In an integrated Risk Management Framework, risk management activities and practices are incorporated into the everyday business as usual activities. These practices work in conjunction with Council's policies, values and culture. The intention is not to "bolt on" risk considerations to existing processes, but to blend in risk considerations in a way that risk is part of the business as usual (BAU) processes and is a value-add activity. Table 3 outlines the areas where risk management practices are incorporated into Council processes.

Table 4: Integration of risk management (see further detail in Risk Procedures)

Key Council Activity	Example Of Where or How Risk Management Is Integrated
Strategic planning	• Risks to achievement of the Council Plan
Project development and oversight (both corporate centre and community initiatives)	• Business case development • Status monitoring and oversight • Milestone reporting

Internal audit plan	IA plan is targeted towards higher rated risks and/or matters of high priority to management.
Procurement	• Value for money considerations • Supplier due diligence • Contract management
Information security	• Information privacy • Protection of data and information systems from cyber threats
Data management	• Model risk • Data validity assessments
Financial management	• Financial Risk Management Framework • Financial delegations based on seniority and job description
Executive and Audit and Risk Committee oversight	• Regular reporting of risk profile and related activities • All papers include assessment against Council's risk appetite statements.
Recruitment and human resources	• Candidate background checks and due diligence • Performance management • Position descriptions
Compliance	• Monitoring of activities against compliance obligations
Business planning	• Financial, capability and delivery risks in change activities
Operational processes	• Design of process steps
Occupational Health and Safety (hazard management)	• Threats to staff and visitor health and safety across Council activities
Business continuity	• Development and testing of plans designed to continue operations in the event of business interruptions
Emergency management	• Development and testing of emergency management procedures
Policy development	• Risk considerations in every policy developed and reviewed
Risk profiling	• Frequent identification and assessment of risks across council activities

3 Design

This Risk Management Framework considers, amongst others, Council's role in the community, its obligations, objectives and business processes, to create a Risk Management Framework that is tailored to suit Council's needs and operating environment (it is fit for purpose). As demonstrated in this document, the Framework has assigned roles

accountabilities and resources for risk management and the channels for risk consultation are described in the separate *Risk Procedures*.

4 Implementation

The Risk Strategy and related timeline outlines the key risk management activities intended to ensure there is an appropriate design, maintenance and application of the framework that is efficient, value add and fit for purpose.

5 Evaluation

Risk management performance is assessed through feedback on the design, execution and outcomes of risk profiling and reporting activities, implementation of risk tools into the business as usual and Human Resources performance management (where appropriate).

6 Improvement

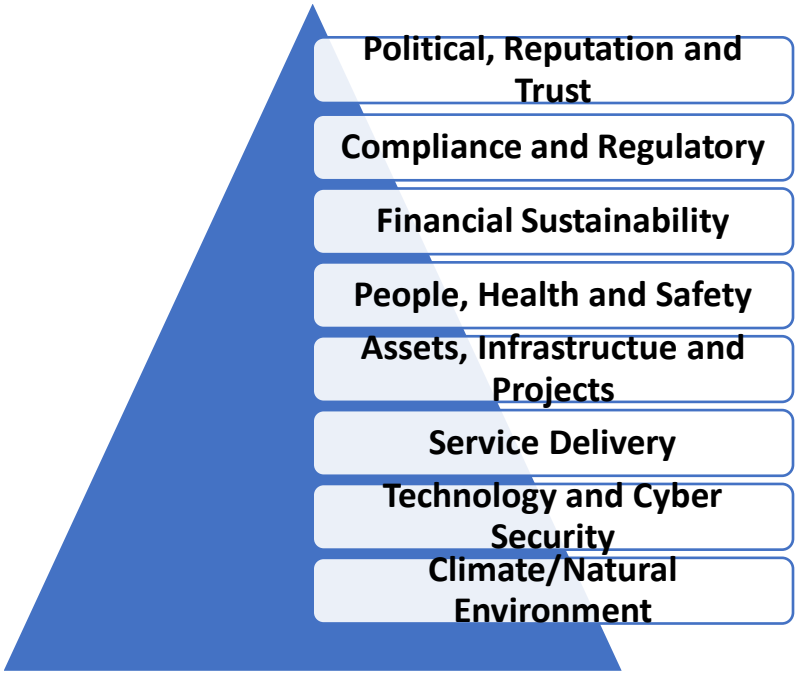
The Risk Management Framework and associated components are reviewed on a periodic basis to ensure they remain current, reflect better practices and are fit for purpose. The Audit and Risk Committee provides endorsement of the Risk Management Framework components outlined in this document.

7. CATEGORIES OF RISK

There is value in analysing trends in risks - it helps management to understand the root cause of weaknesses in Council procedures and controls and helps to direct risk mitigation effort towards the most significant matters.

The categories of risk are a basis for aggregating, analysing and reporting risk trends. Most risks on Council's profile will have a correlation to one or more of the categories below, which align to the risk rating table (see Table 5.)

Figure 4: Council's Categories of risk



Risk Category	Risk Description
Political, Reputation and Trust	Events that impact Council's political stability. Impact to Council of Political outcomes or economic downturns. Reputational risks in the community and through media including social media.
Compliance and Regulatory	Risks that impact compliance with regulatory requirements and legislative obligations.
Financial Sustainability	Financial impact Risks to the Council – Rates and other revenue, unplanned expenses, Management of Assets and Liabilities, reserves and adequate Insurance cover.
People, Health and Safety	Risks that impact the health and safety of staff, contractors and volunteers including OH&S legislative requirements, and public safety risks.
Assets, Infrastructure and Projects	Risks that impact the development of new and redevelopments of existing buildings. Available resources to provide sufficient repairs and maintenance to Council Assets.
Service Delivery	Risks that impact the delivery of critical services to the community due to a business disruption event. This includes services to facilities used by all members of our community, disadvantaged and people of all abilities.
Technology and Cyber Security	Risk of interruption to technology. Damage to Council's core business including cyber-attacks, power outage and other services (Internet), data loss, security breaches or complete systems failure.
Climate/Natural Environment	Risks that impact the local natural environment including Indigenous land and other assets, Impact form hazardous waste and other pollution of water resources, fauna and flora, Impacts from climate change and regular severe weather events.

RISK APPETITE

Risk appetite represents how much risk Council is willing to take on to achieve our strategies and goals. The risk appetite statement (RAS) is a shared understanding of what is acceptable and unacceptable risk taking at Council. This statement helps to avoid personal perceptions and biases that can adversely influence risk-based decisions.

Risk Appetite and Tolerance Statements

Strathbogie Shire Council is committed to building a flourishing community through effective partnerships, engagement, equitable and efficient delivery of services. We aim to create an organisation and a community that is resilient to risk and is prompt to recover in the event of adversity.

To achieve our goals we are prepared to take on measured risk and will do so with informed decision-making practices. We will address uncertainty through open and frank discussions to identify and manage risk and avoid personal perceptions and biases from hindering our

objectivity. We accept that we won't always achieve our goals as planned, but we apply sound risk management processes to the best of our ability to reduce the likelihood and impact of risks becoming loss events.

We will embed risk thinking into our everyday activities to help us to consider what could go wrong, and what must go right, before committing to an action that impacts the better interests of our organisation and our community.

Table 6 documents and sets the risk tone for the organisation.

Table 6: Risk Category - Risk Appetite

Risk category	What is acceptable activity to achieve our strategy? (our appetite for risk)	What is NOT acceptable activity to achieve our strategy? (outside of our risk tolerance)
Political, Reputation and Trust	• Media coverage of the project work in progress • Community concern is voiced locally, key relationships not impaired	• Details of the projects, Financials or other adverse events being advised to the media. • Adverse media coverage leading to Community concern and impacts on key relationships.
Compliance and Regulatory	• Minor breach of in-house policy by individual staff members. • Minor breach of Code of Conduct or Governance Rules by Councillor	• Breach of regulatory requirement at Senior Manager/Executive or Council level.
Financial Sustainability	• Annual budget variances in Council annual operating budget and individual project budgets up to 5% • Inflation and price increases are outside of our control. • Government grants funding allows us to continue delivery of the plan despite being limited by rate capping	• Annual budget variances in Council annual operating budget and individual project budgets >tolerance • Fraud or spending not within the community's best interests • Breach of financial delegations • Purchases made without adherence to procurement policy and controls. • Activity outside of general and administrative expense budget/s
People, Health and Safety	• Minor medical treatment or limited sick leave. • Employing external contractors and SME's to deliver the projects under an agreed value • Annual unplanned staff turnover of 7% (up to 10% is tolerated)	• Under investment in non-medical health and wellbeing services • Injury or illness requiring emergency response or hospitalisation. • Substantial health impact on multiple members of staff

	• Adequate investment in non-medical health and wellbeing activities	
Assets, Infrastructure and Projects	• Asset damage/impact that is planned and approved	• Asset damage that is severe or long term • Buildings without approved fire-retarding materials and sprinkler systems • Buildings without mobility impairment and security facilities • Changes to the built environment that negatively impact the natural environment. • Threats to our heritage buildings
Service Delivery	• Adverse events of a temporary nature including, Covid, Weather, Resource shortages which impact on Regular services to Shire	• Council staff operating without proper authority, training or qualifications impacting on expected levels of Service Delivery • Behaviours or activities within Council or the community that compromise health, safety and wellbeing.
Technology and Cyber Security	• Discreet interruption of <1 day to business unit/s undergoing system change activities • Brief service interruptions	• Serious disruption to system leads to more than 3 days down-time(loss of data and Customer support) • Negative downstream impact on other business units, councils or community groups • Adverse impacts to Payment systems and support services
Climate /Environment (natural)	• Impacts resulting from Council activities are short term, localised and contained. • Accidental spills are quickly rectified and environment restored to natural state. • Minimise impact of Climate Change. • Investment in activities that reduce the impact of environmental impairment	• Widespread spills or long-term impairment emanating from Council activities and construction. • Physical construction without environmental impact assessment • Fire and natural disaster protection measures that are insufficient to prevent or limit the spread of fire/disaster. • Weaknesses in our waste management services that compromise health and safety. • Planting non-native local flora

Risk is a key consideration in all reports to ELT, the Audit and Risk Committee, the project steering committee and Council briefings and meetings.

Every report includes a statement how the matter being addressed, or the decision being requested has been assessed for risk against Council's approved risk appetite statement, where possible.

8. RISK RATING MATRIX

The risk rating matrix is a tool designed to help analyse risks and prioritise them for treatment and reporting. It reflects the materiality of a risk in accordance with pre-defined consequence and likelihood criteria that are aligned to key categories of Council risk.

The matrix is pitched at a Council-wide level to maintain a consistent perspective of risk management across all staff and divisions.

A risk can be aligned on a *best fit* basis to any of Council's *Categories of risk* and does not need to be consistent with all impact statements.

Table 7: Risk rating matrix (image only)

		Consequence				
		Insignificant (Rating 1)	Minimal (Rating 2)	Moderate (Rating 3)	Major (Rating 4)	Catastrophic (Rating 5)
Likelihood	Almost Certain (Rating 5)	Medium (5)	Medium (10)	High (15)	High (20)	High (25)
	Probable (Rating 4)	Low (4)	Medium (8)	Medium (12)	High (16)	High (20)
	Possible (Rating 3)	Low (3)	Medium (6)	Medium (9)	Medium (12)	High (15)
	Unlikely (Rating 2)	Low (2)	Low (4)	Medium (6)	Medium (8)	Medium (10)
	Rare (Rating 1)	Low (1)	Low (2)	Low (3)	Low (4)	Medium (5)
Opportunity (Best Practice/Improvement)		Opportunity (0)	Opportunity (0)	Opportunity (0)	Opportunity (0)	Opportunity (0)

RISK ESCALATION CRITERIA

Risk escalation criteria (as detailed in Table 8 below) is the standard upon which risks must be notified in accordance with the materiality of the risk, as ranked in accordance with the risk rating table. It gives the people deemed accountable for the risk every opportunity to address the risk in a timely manner and reduce the likelihood of the risk becoming an event.

Table 8: Risk escalation criteria

Risk Rating	Overview	Response Time
High	Issue represents a control weakness, which could cause or is causing major disruption of the process or major adverse effect on the ability of the process to achieve its objectives. Requires significant senior management intervention, resource diversion potential and may require possible external assistance. Requires high priority to be actioned.	Immediate - 3 Months
Medium	Issue represents a control weakness, which could cause or is causing moderate adverse effect on the ability of the process to achieve its objectives. Requires considerable management intervention and may require possible external assistance. Requires prompt action.	3 - 6 Months
Low	Issue represents a minor control weakness, which is minimal but reportable impact on the ability of the process to achieve its objectives. Requires management attention and possible use of external resources. Requires action commensurate with the process objectives.	As soon as practical
Opportunity	Issue represents a best practice improvement, which is not addressing an identified risk but looking to improve efficiencies and business practices. Requires review by management with a view to implement if considered practical and beneficial.	As soon as practical

The Risk Profile

Council's risk profile considers (i) the *internal context* i.e., matters emanating from within council activities, and (ii) the *external context,* which are matters influencing Council activities such as state government policies.

The risk team coordinates strategic and operational risk profiling activities on a periodic basis in accordance with documented procedures. Risk assessments pertaining to strategic planning, business planning and project management are conducted on an as-needs basis. Council's risk profile is comprised of:

Strategic risks	Strategic risks are based on council objectives, mission and Council's Strategic Plan and generally occur across most or all divisions and business units in Council effecting such areas as human resources, IT, Security and information management.
Operational risks	Operational risks may be incurred in everyday business activities. For example, financial, business continuity, information privacy, procurement
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.

Risk Register

Operational risks are identified by staff teams and documented with the assistance of the Risk Officer. The system is used by teams at the operational level to record risks, record and monitor treatment activities, assign responsibility for treatments, monitor treatments, record control effectiveness assessments and generate risk reporting. Internal Audit use the Operational Risk Register to help develop the Internal Audit Program.

Strategic and whole of Council risks are recorded in a PowerPoint format and this report is used as the basis for reporting risks to the Audit and Risk Committee and to Council Meetings.

Project Risks are recorded for each project from the inception stage.

Key fields in the risk register are:

- **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?
- **Actions** - 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:

Table 9: 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.

Control Effectiveness

The key purpose of a control is to ensure that processes, procedures, decision or risk mitigation activities operate as expected. For example, an automated control is designed to prevent unauthorised system access every time someone attempts to logon. Failure to enter approved login details into an approved computer will prevent the user from accessing the system.

Controls can be designed to:

- **Eliminate the risk** by stopping the risky activity.
- **Substitute** the risky activity with a *less* risky or alternative activity.
- **Isolate** processes (or people) from the risk
- **Engineer the risk** at its source by redesigning the process.
- **Administer the risk** through policies and procedures.
- Provide protection through **personal protective equipment** (for safety purposes only)

Control Categories

Controls can be categorised as follows:

a) Preventative Controls - controls that prevent the risk event from occurring. For example, a computer's financial software controls prevent financial payments being processed through a computer system until appropriate system password access controls prevent unauthorised access to a function or system.

b) Detective Controls - controls designed to identify risk events once they have occurred. For example, a reconciliation that is designed to identify differences between systems or account balances.

Preventative controls are generally more appropriate for high impact loss events whereas detective controls are generally more effective for low impact/high volume risks.

Controls are effective when:

1. The control design appropriately addresses the risk (in this case the risk of unauthorised access), and
2. The control works as expected every time (in this case the computer system automatically applies password access requests prior to granting system access).

However, not all controls are automated and may not always be fully effective. This is particularly relevant where a specific human action is required, and by nature this is subject to the reliance of the human operating that control fully and in accordance with the control design, every time. For example, this may be a manual reconciliation of accounts or checks that equipment is tied down or stored away securely prior to transportation.

An assessment of control effectiveness across a division or category of risk can identify targeted control weaknesses or underlying cultural issues. For example, a series of control review status not updated/reported on or requiring improvement for a long period may indicate a risk awareness or risk accountability issue in the first line. This is a trigger for further risk mitigation activity.

Accountability for control effectiveness sits with the first line of defence. Responsibility to undertake this may be undertaken by management or delegated to the second or third line functions.

Control operating effectiveness is categorised as follows:

Effective	Controls are appropriately designed to mitigate the risk to an acceptable level. Controls address the root causes and management has strong evidence that controls are working reliably as expected.
Adequate	Controls are designed appropriately to mitigate risk to an acceptable level. The control is monitored on an ad hoc basis and evidence indicates the control should be working as expected.
Improvement Required	While controls are largely addressing root causes of the risk, evidence indicates the controls are not fully implemented or are not operating reliably and hence risk is not being reduced to an acceptable level. Additional work is required to improve control implementation and reliability.
Poor	Reviews on control effectiveness are limited or are not performed. Where available, evidence indicates that risk mitigation strategies are not working as expected due to poor control design and/or limited operating effectiveness.

9. RISK CULTURE

Council's risk culture does not sit separately from the organisational culture. It is a component of the organisational culture that illustrates how risk awareness, accountability and attitudes are applied at Council. Risk culture takes the inherent values and beliefs of individuals and translates this through the Risk Management Framework into risk behaviours that reflect Council's attitude for risk.

Embedding risk behaviour into process mechanisms leads to a sustainable risk culture. It enables us to confidently perform daily operations and make informed decisions knowing that the risks impacting our work have been rigorously assessed and appropriately mitigated.

However, with changes in strategic direction, organisational priorities, funding availability and inevitable turnover of staff, risk values and capability can often be eroded. To mitigate this risk, Council's approach is to embed risk culture into the mechanisms of our operating environment to help ensure risk behaviours are repeated, sustained and positively impact our organisation and community (see Figure 5 below).

A staff survey assesses how well risk management is understood and applied at Council. Risk culture at Council is also evident through our:

- Charters and terms of reference
- Meeting minutes
- Induction and training programs
- Position descriptions
- Performance reviews
- Risk profiling agendas and participation
- Audit programs
- Risk recording and reporting

Figure 5: Components of Council's risk culture

Audit and Risk Committee

Council's Audit and Risk Committee maintains oversight and guidance of the risks impacting our everyday activities. The Committee receives reports on the effectiveness of the Risk Management Framework which includes risk culture. Risk Management is everyone's responsibility and this is endorsed through the CEO, the Executive, our policies and this framework document.

Training And Awareness

Risk management training is included in induction of new staff, further training being conducted on an as-needs basis, such as following a change to procedures or reporting requirements. The regular risk-profiling forums are an appropriate medium for training staff and sharing risk information. However, training alone is not sufficient to ensure risk culture and capability is integrated into the business as usual.

Integration And Accountability For Risk In Our Processes

Regular team meetings include the identification of new or changed risks as an agenda item. In addition, each team conducts an annual meeting devoted to risk in their area. At the annual meeting, the teams review the current risk register for their area and identify any new or changed risks

Risk is also considered in the development of policies such as procurement, privacy, conflict of interest, through procedures such as accounts payable and receivable, and through mechanisms such as financial delegations. Our position descriptions include accountability for risk. This helps to embed awareness and responsibility for managing risk and shapes our organisational risk behaviours.

Through the application of organisational-wide operational procedures and controls, risk management practices and behaviours are applied consistently and the need to rely on individual judgement is minimised.

Risk Engagement

The Executive Leadership Team (ELT) is central to embedding risk into daily activities and to promoting staff engagement in ongoing risk discussions. They role model risk behaviours and risk language, and encourage openness and transparency in risk discussions, escalation and reporting. This approach helps to promote and sustain a common and shared understanding of risk throughout Council.

Annual Risk Calendar

The freedom to record, report and openly discuss risks without fear of blame or reprisal is a key measure of our attitudes towards risk at Council. This attitude is reflected in our risk appetite statement.

We have scheduled opportunities to discuss risk matters in an open and transparent environment, and independent reporting lines to the Risk Officer allow staff to raise risk concerns in confidence where required:

- Our annual risk profiling sessions are forums for raising risk concerns and staff have the option to discuss risk in confidence as needed with the Risk Officer.
- The Risk Officer has a "dotted" reporting line to the Director People and Governance on risk matters and has the opportunity to raise risk concerns *in camera*.

Reporting Requirements

Under the Local Government (Planning and Reporting) Regulations 2014, Council is required to generate *"six-monthly reports of strategic risks to Council's operations, their likelihood and consequences of occurring and risk minimisation strategies".*

Risk reports are designed to help management address uncertainty and aid decision-making. By understanding what could go wrong and what must go right, management can determine a course of action to effectively manage risk.

Operating Team Level

An annual zero-based review of potential risks to the operations of teams is conducted in March each year.

At monthly team meetings Teams will review the following:

- Emergence of new risks
- Occurrence of any risk events
- Treatment of the above.

Executive Leadership Team Level

In April each year ELT will review the operational level risks arising from the operating team level.

In October each year ELT (and broader management team if required) will conduct a zero-based review of Strategic and Whole of Council Risks.

At Project Portfolio Review Meetings ELT consider the risks associated with each project.

At monthly ELT meetings ELT will review the following:

- Emergence of new Strategic risks;
- Occurrence of any Strategic risk events;
- Any Operational or Project Risks identified; and
- Treatment of the above.

Audit and Risk Committee

At each Audit and Risk Committee Meeting the Committee will receive a report which addresses key performance indicators relating to Strategic and Project Risk. The report identifies any occurrence or increased likelihood of strategic risk events, any mitigations undertaken, and progress on actions scheduled to mitigate strategic Risks.

In June and December each year the Audit and Risk Committee will receive a report on the agreed Strategic Risks to Council plans, their likelihood and consequences of occurring and our risk mitigation strategies.

Council

In February and July each year Council will receive a report for their review and acceptance on Council's Strategic Risks, their likelihood and consequences of occurring and risk mitigation strategies.

In February each year, Council will review the risk appetite and tolerances for the organisation and revise as required.

Appendix A: Reconciliation - Principles of the Risk Management Framework

This Risk Management Framework is founded upon the International Risk Management Standard – ISO 31000: 2018 (the Standard). The nine principles from the Standard are the characteristics of effective risk management and is the basis upon which risk is managed at Council.

The table below reconciles the nine principles in the standard ISO 31000:2018 against Council's application of the principle:

Table 8 - Risk principles reconciliation

Principle	Council's Application
1. Creates value and protects assets	The objectives of risk management at Council are outlined in this document, section: *Objectives for Council's management of risk.*
2. Is integrated into Council's daily activities	Per the key processes listed in this document, section: *Integration of risk into Council activities.*
3. Is structured and comprehensive	This framework outlines the structure for managing risk across the key Council processes.
4. Is customised to Council's internal and external context	Risk management activities reflect Council's operating environment, reporting lines, governance structure, key stakeholders and cultural environment and is cognisant of risk management capacity and capability.
5. Is inclusive of a range of perspectives from key stakeholders	Periodic strategic and operational risk profiling, risk reporting and oversight activities capture a range of risk perspectives from a range of staff.
6. Is dynamic and is responsive to organisational change	Risk integration and profiling activities are dynamic and scheduled to align with key activities in Council's business cycle (e.g., profiling scheduled to assist in development of the Council strategy and annual business plan).
7. Is based on best available information	Risk information is based on the contemporary views of key stakeholders, research and advice and is applied to ERM processes such as risk identification and profiling activities and maintenance of the Risk Management Framework.
8. Takes human and cultural factors into consideration	Risk culture is a subset of Council culture. This framework is a consensus view of how risk is managed at Council.
9. Facilitates continual improvement through learning and experience	The risk strategy outlines Council's approach to ongoing risk improvement activities.

Appendix B - Risk Rating Matrix

		Consequence				
		Insignificant (Rating 1)	Minimal (Rating 2)	Moderate (Rating 3)	Major (Rating 4)	Catastrophic (Rating 5)
Likelihood	Almost Certain (Rating 5)	Medium (5)	Medium (10)	High (15)	High (20)	High (25)
	Probable (Rating 4)	Low (4)	Medium (8)	Medium (12)	High (16)	High (20)
	Possible (Rating 3)	Low (3)	Medium (6)	Medium (9)	Medium (12)	High (15)
	Unlikely (Rating 2)	Low (2)	Low (4)	Medium (6)	Medium (8)	Medium (10)
	Rare (Rating 1)	Low (1)	Low (2)	Low (3)	Low (4)	Medium (5)
Opportunity (Best Practice/Improvement)		Opportunity (0)	Opportunity (0)	Opportunity (0)	Opportunity (0)	Opportunity (0)