Enterprise
Risk Management Framework

Date Adopted: 24 October 2023
Resolution No. 179/23.
Version: 2
Review date: October 2023

Contents

Context

Effective risk management is fundamental to achieving our purpose, improving our performance and achieving value.

Risk is inherent in all of George Town Council (Council) activities. Council recognises that risk is inherent in carrying out all its business strategies and operations and that without a robust system for identifying and managing risks, the organisation is vulnerable to uncertainties and lost opportunities and is unlikely to be resilient in the face of change or adversity.

Council cannot provide the services that the community and public need without being exposed to risk which has both positive aspects (opportunities) as well as negative aspects (threats).

To make the most of opportunities, limit negative impacts, and enable considered decision-making, we identify, assess and manage risk through our Enterprise Risk Management Framework (RMF).

The RMF sustains a proactive and ongoing engagement with risk and an understanding that helps foster a positive risk culture, that while cognisant of managing risk to the lower ranges, also encourages experimentation, acceptance of some risk, and tolerance of mistakes or adverse outcomes. A positive and proactive risk culture also helps shape Council's strategic direction, contributes to strategy, and embeds aligned thinking into decision-making and business-as-usual practices. In turn, our risk culture is sustained through workplace behaviours, decision-making attitudes, and alignment with all the Council's values, particularly accountability, innovation, respect, and transparency.

Integrated and effective application of the RMF is also a primary enabler of the Council's ability to operate in a way consistent with the *Local Government Act* (1993) and other legislation. It also underpins community trust and confidence in our ability to achieve the outcomes expressed in the Community Strategic Plan 2020-30, and to enable the delivery of actions in the annual operational plans, particularly those objectives focused on leadership, resilience, organisational sustainability, and accountable governance.

Purpose

Risk management is a shared responsibility for all elected representatives, employees, and contractors. In line with this responsibility, the RMF sets out why and how we undertake risk management.

The RMF is the primary source of guidance for managing both strategic and operational risk. The framework has been designed to support employees to understand:

- How the Council identifies, responds to, and manages risk.
- The connection between the components that make up the RMF (such as the Risk Management Policy and Framework, Enterprise Risk Register and Risk Procedures); and
- Their responsibility to manage risk as part of their everyday decision-making processes.

Through application of the RMF, Council aims to achieve an environment where, with the provision of ongoing guidance and training, Council staff retain the risk management skills to effectively contribute to the pursuit of objectives, whilst endeavouring to protect the Council, its staff, its community, key stakeholders and natural and constructed assets from the adverse effects of risks.

Application of the RMF will assist Council to:

- Appropriately achieve its goals and the outcomes expressed through strategies and plans.
- Protect the safety of people, assets and finances and the Council's reputation.
- Assess and take considered risks in accordance with approved policies and values.

- Adopt risk treatment activities that are fit for purpose, cost effective and are designed to reduce risk to an acceptable level.
- Embed a culture that promotes awareness and accountability for risk, so it becomes a normal way that business is done at Council.

Scope

The RMF applies to all levels of the organisation - Council staff, management, Councillors, key stakeholders, contractors, and service providers. It extends to all of Council's current and future strategic and operational activities, business practices, policies, strategies, plans and procedures, as well as new opportunities for the organisation and the community.

Review

The RMF is reviewed biennially, while the appetite for risk is reviewed annually as part of the annual planning and budget cycle.

The risk register is a 'live' document that is continually updated to reflect our risks and operating environment. The framework and register are regularly reported on to the General Manager, Council and the Audit Panel. The ongoing approach to monitoring risk enables Council's senior leadership team to implement mitigation plans and introduce additional controls to bring enterprise risks rated above our tolerance levels back to an acceptable level.

Governance and oversight

Council's risk governance structure is aligned to the organisational structure. It represents the accountability and responsibility for risk, reporting lines for risk information and the path for risk escalation and verification of compliance to policy and process.

It starts with Councillors and cascades through management and all levels of staff. Independent oversight of risk is achieved through the Audit Panel and assurance via the internal audit function.

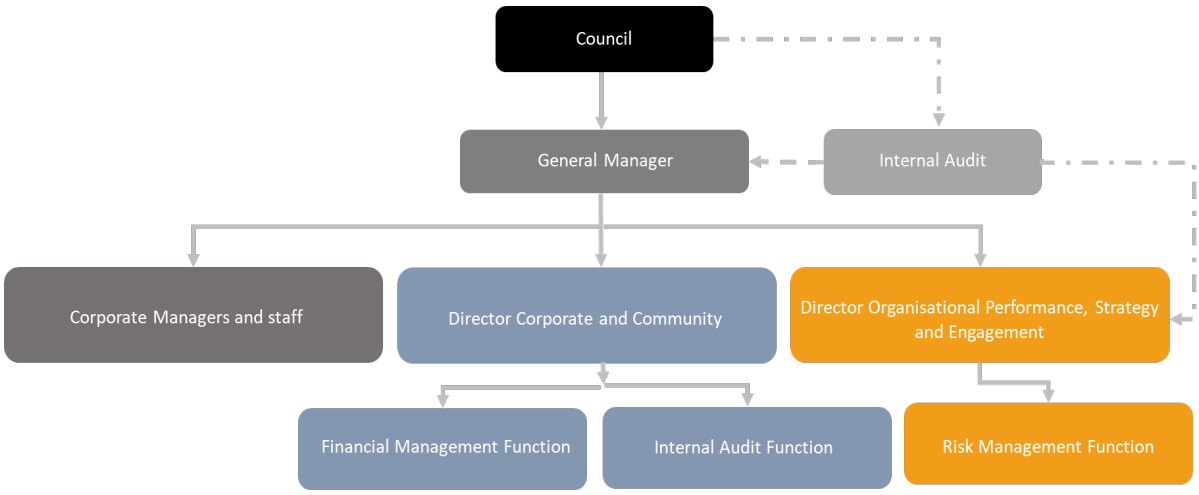


Figure 1: Council's Risk Management Governance Structure

Roles, responsibilities and accountabilities

The RMF and its implementation is the responsibility Director, Organisational Performance, Strategy and Engagement. The roles and responsibilities for risk management at Council are specified in this policy, committee charters and individual position descriptions.

Figure 2: Roles and Responsibilities for Risk Management

Overview of risk documents

The George Town Council RMF is the totality of all documents, processes, systems and personnel that operate the framework for the purposes of risk management at Council and includes the following component documents and processes:

1. Risk Management Policy

The policy defines our organisational approach to risk management and links the RMF to our purpose, strategic planning framework and objectives. In addition, the policy defines Council's enduring strategic risk appetite and risk tolerance; and contains an outline of the key accountabilities and responsibilities for managing and implementing the RMF.

Approval: Council.

2. Risk Appetite Statement (RAS)

The RAS deals is a set of statements that describes Council's attitude towards risk taking. The RAS focuses on two aspects; risk appetite and risk tolerance (see definitions). Risk appetite sets the tone for risk taking in general, whilst tolerance informs:

- Expectations for mitigating, accepting and pursuing specific types of risk.
- Boundaries and thresholds of acceptable risk taking.
- Actions to be taken or consequence for acting beyond approved tolerances.

Council decision makers and employees will use the RAS:

- When developing and applying Council's risk register and actions to mitigate risk.
- In the decision-making activities of Council. Activities including financial planning, projects, strategic and operational planning, governance arrangements, performance management, regulatory oversight, program and policy design and implementation are to be managed within range of acceptable appetite and tolerances set out in this document.

Approval: Council.

3. Enterprise Risk Register (ERR)

The RMF is supported by the ERR which identifies, outlines and assesses relevant strategic and operational risks across Council. The ERR is a 'live document' that is reflective of the current risk mitigation and control measures.

The ERR is maintained by Corporate Services & Finance with contributions from all departments. The ERR is maintained and reviewed along with actions to mitigate risk at least every six months or when there is a material change to circumstance or business capability that compels re-assessment. The ERR is periodically tabled at workshop to the Council and Audit Panel.

Approval: General Manager.

4. Risk Procedures

The risk procedures guide and support a consistent approach to risk management across Council and explains how to undertake risk management in line with International Standard ISO31000:2018, Risk management – Guidelines. Each step in the ISO31000:2018 process is outlined in detail along with descriptions of how and where the process is applied by Council.

Approval: General Manager.

5. Audit Panel Charter

Council's Audit Panel provides an independent mechanism to review and advise on Council processes and decision-making, including those relating to the management of risk. The Audit Panel Charter sets out the role, function and requirements for the operation of the Audit Panel.

While the development and implementation of the RMF is the responsibility of the Council, the Audit Panel has a key role in overseeing and monitoring its effectiveness and application.

Approval: Council.

Principles, framework and process

Council's approach to risk management is aligned to the International Risk Management Standard – ISO 31000: 2018 (the Standard) and tailored considering 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 management throughout Council.
- Helps Councillors and employees to discharge their duties and responsibilities.

Council recognises the need to apply the principles and processes detailed in AS/NZS ISO 31000:20018 Risk Management - Guidelines to ensure the management of risk in an efficient, effective and consistent manner.

As represented in the diagram below, the Standard provides nine principles of effective risk management which inform both process and the overall risk management framework and necessary leadership support. The nine principles give a structured approach to the management of risk that when consistently implemented, allows risks to be identified, analysed, evaluated and managed in a uniform and focused manner.

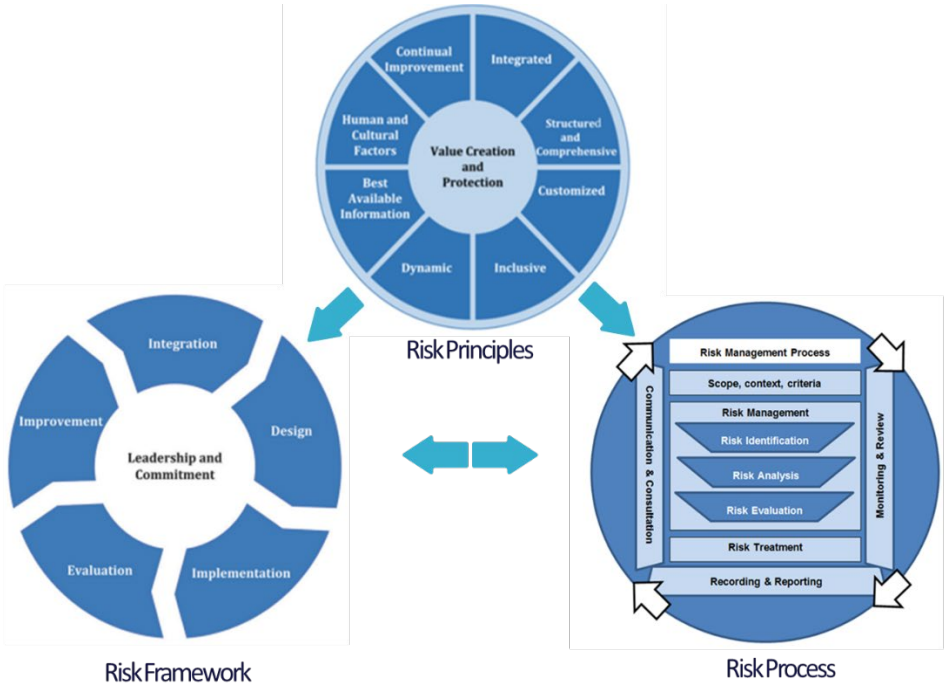


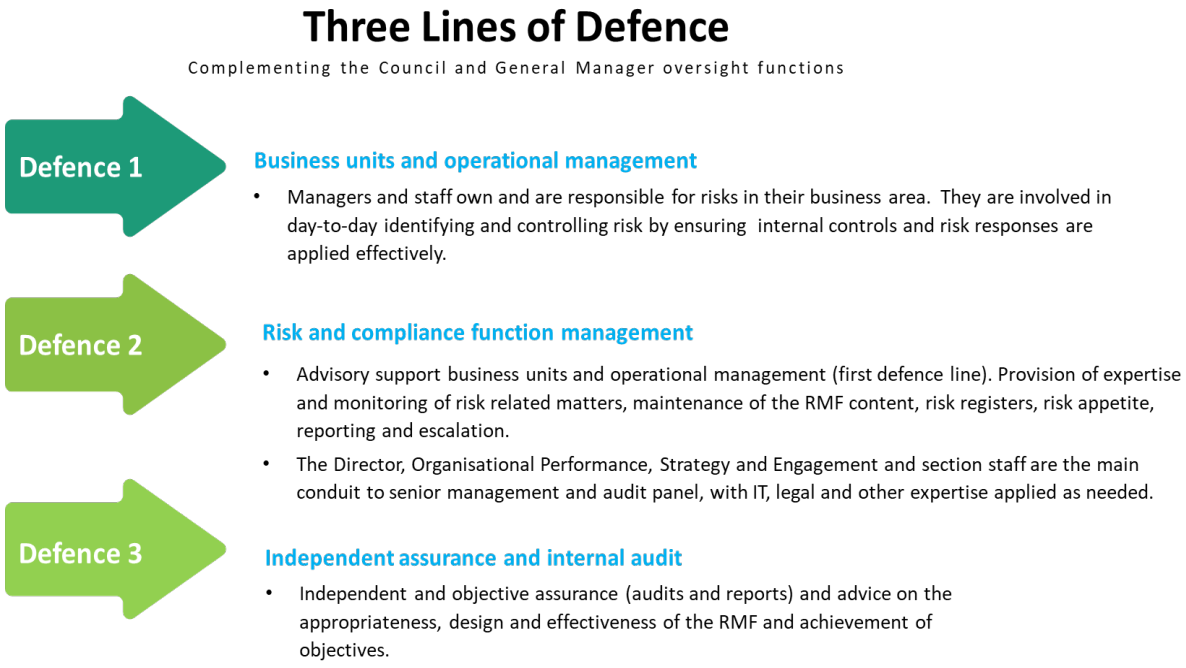
Figure 3: Framework, Principles and Process Integrate across Council Business (Source ISO31000:2018)

Through the implementation of an integrated and consistent approach to risk management, Council aims to achieve the following risk management objectives:

- An organisational culture of reliable, informed, evidence-based planning and decision making.
- A consistent approach to the identification, assessment and treatment of risks.
- Improved communication on matters of risk to enhance decision making.
- Proactive and adaptive management practices.
- Support achievement of Council's strategic objectives.
- Effective allocation and use of resources for risk treatment.
- Enhanced identification of opportunities and threats
- Enhanced organisational resilience and continuity of service.
- Improved operational effectiveness and efficiency.
- Staff accountability for risk identification and treatment
- Improved corporate governance, controls and performance.
- Improved community and stakeholder confidence and trust by providing assurance that risks are appropriately managed.
- Reduced liability exposure and financial loss.
- Safeguarding of Council's resources - its people, finance, property and reputation.

The three lines of defence

Council operates a 'three lines of defence' (3LOD) model to actively manage, monitor and oversee risk and the implementation of related policy and procedures. As represented below, this model comprises:



Risk management process overview

The Risk Management Process is the systematic application of management policies, procedures and practices to the tasks of establishing context, identifying, analysing, evaluating, treating, monitoring and communicating in relation to risk. Council will apply the following process as defined by AS ISO 31000:2018 Risk Management - Guidelines:

Figure 4: Risk Process. Source: ISO31000:2018.

Consistent with the above schematic of the risk management process, the risk procedures are undertaken and documented using Council's risk assessment templates and criteria with practical

assistance from staff within Organisational Performance, Strategy and Engagement, however a basic overview of the process is presented in the table below:

Step	Process	Description
1	Communication and consultation	• Communication and consultation with relevant internal and external stakeholders undertaken at all stages of the risk assessment process to bring different areas of expertise together, ensure different views are appropriately considered, to provide sufficient information to facilitate risk oversight and decision making, and to build a sense of inclusiveness and ownership among those affected by the risk. • This step involves promoting awareness and understanding, as well as seeking feedback and information to support decisions made throughout the process.
2	Setting the scope, context and criteria	• This step is undertaken to gain an understanding of the purpose of the risk assessment and factors that may require consideration throughout the process. • Risk analysis includes defining the scope of the activity being assessed, the relevant objectives to be considered and any relevant relationships to other projects, processes and activities; desired outcomes from the steps to be taken; decisions that need to be made; the internal and external environment; resources required and associated responsibilities; the risk assessment criteria, tools and techniques to be applied and the records to be kept throughout the risk assessment process.
3	Risk Assessment: the risk assessment process involves the following three steps:	
	Risk Identification	• Identifying risks involves consideration of what, how, why and when events might occur that could have an impact on achieving the objectives of the activity or operation being assessed. • During this process consideration is given to Council's adopted Risk Categories. A variety of methods can be used to identify risks, such as brainstorming and SWOT analysis. Relevant, appropriate and up to date information is important to identifying risks.
	Risk Analysis	• Risk analysis is undertaken to determine and understand the level of risk being faced. It involves a detailed consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness. • Risk analysis provides input to risk evaluation, decisions on whether risk needs to be treated and how, and on the most appropriate risk treatment and methods. • Risk analysis is undertaken using Council's adopted Risk Assessment Criteria.

Step	Process	Description
	Risk Evaluation	• The purpose of risk evaluation is to support decisions. It involves comparing the results of the risk analysis with the Council's established risk criteria to determine if the level of risk is acceptable or additional action is required to continue with the activity or operation being assessed. • Options may be to do nothing; consider risk treatment options; undertake further analysis; maintain existing controls; reconsider objectives; and it should consider the wider context and the action and perceived consequences to both internal and external stakeholders.
4	Risk Treatment	• Risk Treatment involves the development and implementation of additional controls, such as systems and procedures, to address the risk. Risk Treatment involves an iterative process of formulating and selecting risk treatment options; planning and implementing risk treatment; assessing the effectiveness of the treatment; deciding on whether the remaining risk is acceptable and if not acceptable, taking further treatment. • Depending on the activity or operation that is being assessed and the priority of the risk, risk treatment strategies can involve the development and implementation of long- or short-term risk treatment action plans. Risk Evaluation (Step 3) and Risk Treatment (Step 4) should be undertaken with consideration of Council's adopted risk appetite.
5	Monitoring and Recording	• Monitoring and review of the risk management process, its implementation and outcomes ensures its continued quality and effectiveness and identifies opportunities for improvement. • This step will ensure that identified risks and controls remain relevant, controls remain effective and that any new risks are appropriately identified, recorded and managed appropriately. This should be a planned and documented part of each stage of the process and associated responsibilities should be clearly defined.
6	Recording and Reporting	• The risk management process and its outcomes are required to be documented and reported regularly to ensure continued communication in relation to risk management activities and outcomes, to provide information for decision-making, to improve risk management activities and to assist interaction with stakeholders.

Table 1: Process Relationships to the Risk Management Framework

Building a risk management culture

Council will effectively communicate and engage with staff at all levels of the organisation to build a positive risk aware culture that encourages all staff to proactively manage risks. Council will do this by:

- 'Setting the tone at the top' ensuring Council's leadership promote and commit to risk management in a positive and proactive manner and communicate this with all staff.
- Communicating risk management roles and responsibilities.
- Providing risk management support, ongoing guidance and resources to staff, including easily accessible risk management tools and systems.
- Integrating risk management into strategic and business planning processes.
- Participating in sector wide audits and regional risk initiatives.

Enabling through education and training

Council will facilitate and tailor risk management training for staff to ensure it is relevant to different levels of the organisation and engaging with staff about the benefits of risk management. Risk management training will be conducted as time and budget permits; however guidance will be provided on an ongoing basis by the Director and staff of Organisational Performance, Strategy and Engagement.

Council's training and guidance will include providing staff with the following:

- A general understanding of the principles and benefits of risk management.
- Practical guidance in undertaking and documenting the risk assessment process, using Council's adopted risk assessment and evaluation criteria, tools, templates and systems.
- An understanding of Council's risk appetite and actions required to effectively consider risk management options.

Integration of risk into Council activities

Figure 5: Risk framework. Source: ISO31000:2018

1. Leadership and Commitment

Accountability for risk is promoted through the Councillors, General Manager, Audit Panel and Corporate Management Team and endorsed through the Risk Policy and the RMF. 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 RMF.

2. Integration

In an integrated risk management framework, risk management activities and practices are incorporated into both strategic and everyday business as usual activities.

Council will integrate risk management into its strategic and operational functions. Organisational strategies, plans and programs are to be aligned to this framework so that risk practices can 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 management becomes part of Council's business as usual (BAU) processes and is a value-add activity. Further, it shares accountability throughout Council and avoids the staff within Organisational Performance, Strategy and Engagement from being seen as the people solely responsible for risk management.

Table 2 below provides examples of where and how risk is integrated across Council's business.

Key Council activity	Where or how risk management is integrated
Strategic planning	• Profiling risks to the achievement of the Council plans.
Project development and management (both corporate centre and community initiatives)	• Business case development. • Status monitoring and oversight. • Milestone reporting.
Internal auditing	• IA plan is targeted towards higher-rated risks and/or matters of high priority to management.
Procurement and contract management	• Value for money considerations, supplier due diligence, contract specification and management.
Information security and privacy.	• Information privacy - protection of data and information systems from cyber threats.
Data management	• Model risk and data validity assessments.
Financial management	• Financial risk management framework, financial delegations and job description.
Executive and audit panel oversight	• Regular reporting of risk profile and related activities. • All papers include assessment against Council's risk appetite statement.
Recruitment and HRM	Candidate background checks and due diligence. Workforce planning and performance reviews.

Key Council activity	Where or how risk management is integrated
	Compliance with industrial law.
Regulatory compliance and environmental management	Monitoring of activities against compliance obligations.
Strategic and operational business planning	Financial, capability and delivery risks in change activities.
Operational procedures	Design of process steps (often denoted in process maps).
Occupational Health & Safety (hazard management)	Threats to staff and visitor health and safety across Council activities.
Business Continuity and Disaster Recovery	Development and testing of plans designed to continue operations in the event of business interruptions.
Asset management	Lifecycle and condition assessment, investment prioritisation.
Emergency management.	Development and testing of EM procedures.
Policy	• Risk considerations in every policy developed and reviewed.
Risk profiling	• Frequent identification and assessment of risks across council activities.

Table 2: Integration of Risk Management

3. Design

This RMF considers, amongst others, Council's role in the community, its obligations, objectives and business processes, to create an RMF that is tailored to suit Council's needs and operating environment (it is fit for purpose). As demonstrated in this document, the RMF 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 Program of Work 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 BAU and HR performance management (where appropriate).

6. Improvement

The RMF and associated components are reviewed on a periodic basis to ensure they remain current, reflect better practices and are fit for purpose.

The Audit Panel provides endorsement of the RMF components outlined in this document.

Key risk categories

Council will undertake risk management with due consideration of the following adopted key risk categories:

Figure 6: Council's Categories of risk

Risk appetite and tolerance

Risk appetite is the amount of risk Council is willing to accept or retain to achieve its objectives. It is expressed as statement or series of statements that describes Council's attitude towards risk taking.

Council's risk appetite is captured within the Risk Appetite Statement (RAS).

The RAS will be reviewed every two years as part of the budget development process to ensure assessment of initiatives and proposals against the levels of acceptable risk across relevant risk domains. Reviews are also to be undertaken within four months of a local government election, or as otherwise prompted by a significant change in the operating or environmental circumstance of GTC.

The Council is responsible for approving the RAS, while the Audit Panel is responsible for monitoring and reviewing the appropriateness of the RAS in the context of the Council's overall RMF.

The General Manager and Directors are responsible for reviewing, monitoring, and managing risk within and across their respective Departments in line with the RAS. They are to facilitate risk awareness and embed risk management into day-to-day and formal decision-making.

All staff have a responsibility to escalate for approval any significant or material change to existing risk or additional risk to the business or outcomes of Council.

Decisions of Council are to be informed by consideration of risk and the tolerance of risk as expressed in the RAS. Necessary consideration is achieved by assessment of risk as part of the briefing note and decision paper presented to the Council.

Every paper 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.

Risk tolerance

The RAS also addresses Council's risk tolerances.

Risk tolerances are set against each of the strategic objectives and represent Council's attitude towards risk. This comprises:

- The risk posture that reflects Council's appetite for risk (zero, low, moderate or high); and
- A series of statements that define what is acceptable and what is not acceptable in pursuit of the strategic objectives.

In turn, the risk tolerance influences the approach Council takes with a particular risk and related decisions, ranging from confident to highly cautious. Figure 7 provides a template to assessment of tolerance, with the view to reflecting the circumstances in the RAS.

Strategic objective	Risk posture		Risk tolerance	
	Lowest tolerance	Highest tolerance	What we will accept in pursuit of this objective	What we won't accept in pursuit of this objective
Sample strategic objective 1			• Sample acceptable criteria	• Sample unacceptable criteria
Sample strategic objective 2			• Sample acceptable criteria	• Sample unacceptable criteria
Sample strategic objective 3			• Sample acceptable criteria	• Sample unacceptable criteria
Sample strategic objective 4			• Sample acceptable criteria	• Sample unacceptable criteria
Sample strategic objective 5			• Sample acceptable criteria	• Sample unacceptable criteria

Figure 7: Risk Tolerance Assessment Method

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.

Further detail on the risk rating matrix and its application can be found in the Risk Management Procedures.

CONSEQUENCE	RISK CATEGORY	IMPACT	LIKELIHOOD	RARE May occur once a decade	UNLIKELY May occur in five to ten years	POSSIBLE May occur within five years	LIKELY May occur within months	ALMOST CERTAIN May occur within weeks
CATASTROPHIC	Community & govt. reputation Financial People, safety Compliance Environment Assets, security & infrastructure Business interruption	Community, State Government and media outrage, key relationships broken down Financial impact >$500k Fatality or permanent disability Regulatory investigation, legal action, fines and penalties imposed Uncontrolled spread of toxic pollutants Building destroyed and BCP invoked Critical system failure, business interruption to exceed 1 month in a BCP/DR environment		High	High	Extreme	Extreme	Extreme
MAJOR	Community & govt. reputation Financial People, safety Compliance Environment Assets, security & infrastructure Business interruption	Widespread community concern, adverse media coverage, key relationships severely damaged Financial impact $250k - $500k Injury or illness requires emergency response, hospitalisation Reportable breaches and regulatory investigation at Council level Spread of toxic pollutants is widespread Building severely damaged, partial destruction, denial of access, BCP invoked Systems downtime is widespread and expected to last up to one month in a BCP/DR environment		Medium	High	High	High	Extreme
MODERATE	Community & govt. reputation Financial People, safety Compliance Environment Assets, security & infrastructure Business interruption	Well publicised community concern, limited media coverage and some key relationships strained Financial impact $20k - $250k Injury or illness requires prompt first aid, medical treatment and sick leave Breach of regulatory requirement at Council level Spread of pollutants is broad but controlled Building damage creates a danger to employees or public in immediate vicinity Systems interruption expected to last up to one week. BCP/DR is invoked		Medium	Medium	Medium	High	High
MINOR	Community & govt. reputation Financial People, safety Compliance Environment Assets, security & infrastructure Business interruption	Community concern is voiced locally, key relationships not impaired Financial impact $50- $20k Injury or illness requires minor medical treatment , limited sick leave In-house policy breaches by individual staff members Spread of pollutants is localised and contained Asset damage or interruption creates a limited inconvenience Limited loss of service for up to one day. BCP/DR is not invoked		Low	Medium	Medium	Medium	High
INSIGNIFICANT	Community & govt. reputation Financial People, safety Compliance Environment Assets, security & infrastructure Business interruption	Negligible community concern and impact to public image Financial impact <$5k Insignificant injury, no first aid or sick leave Minor breach of in-house policy by individual staff members Spread of pollutants is minimal or tightly contained Asset damage or interruption is negligible and subject to routine maintenance Brief system interruption, negligible impact on processes		Low	Low	Low	Medium	Medium

Figure 8: Risk rating matrix (image only) - see detail in Risk Management Procedures

Risk escalation criteria

Risk escalation criteria 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.

	Risk tolerance and escalation	Risk treatment and monitoring
Extreme	Risk is far outside of tolerance levels. Escalate immediately to executive management.	Requires immediate treatment to commence within 1 week, with ongoing executive oversight.
High	Risk is outside of tolerance levels. Escalate promptly to senior management.	Requires prompt treatment to commence within 2 weeks, with ongoing senior management oversight.
Medium	Risk is on the tolerance boundary. Escalate to management.	The treatment plan is to commence within 4 weeks with regular oversight from senior management.
Low	Risk is within tolerance boundaries only.	Treatment options and oversight plan to be developed with management.

Table 3 - Risk Escalation Criteria

The risk profile

Council's risk profile considers the *internal context* i.e. matters emanating from within Council activities, and 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.
Corporate risks	Operational risks may be incurred in everyday business activities, in a single department or broadly across Council. For example: financial, business continuity, information privacy, procurement.
Emerging risks	Emerging risks are not currently on the risk register but could become risks, and as such require periodic monitoring and review.

Risk register

Council's risk profile is currently recorded in the Pulse Risk Register System that is operated and maintained by Organisational Performance, Strategy and Engagement. Pulse is used to record risks, record and monitor treatment activities, assign responsibility for treatments, monitor treatments, record control effectiveness assessments and generate risk reporting. 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?
- 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:

Decision	Indicators
Avoid the risk	Decide not to proceed with the policy, program or activity or choose an alternate means of action.
Accept the risk	Council has made a conscious 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 moderate or above are accepted, justification of acceptance is required, and a record included in the relevant 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 take on risk to achieve desired outcomes (of a strategy, project or initiative).

Table 4 - Risk Treatment Options

Refer to the *Risk Management Procedures* for further detail on the risk profile review process.

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:

a) The control design appropriately addresses the risk (in this case the risk of unauthorised access), and

b) 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 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.

Table 5- Control Effectiveness Ratings

Risk culture

Council's risk culture does not sit separately or alongside 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 RMF 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 9 below).

Risk culture at Council is evident through our:

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

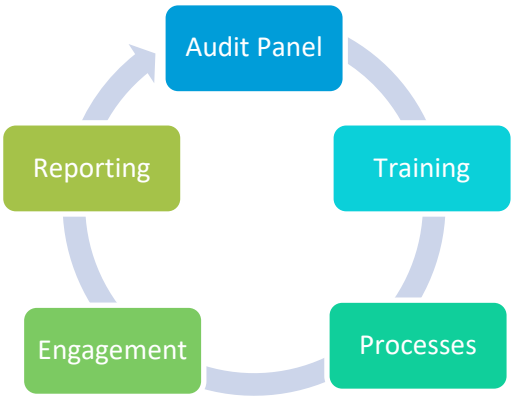


Figure 9: Components of Council's Risk Culture

Audit Panel and tone from the top

Council's Audit Panel maintains oversight of the risks impacting our everyday activities. The Panel receives reporting on the effectiveness of the risk management framework which includes risk culture. The Panel sets the tone for risk management and implements this through the General Manager, Corporate Managers, our policies and frameworks.

Training and awareness

All staff undertake risk training in their induction training, some have heightened levels of training in accordance with their employment conditions. Training includes raising awareness of our framework, the processes for incorporating risk into our everyday thinking and activities, the open and transparent way in which we consider risk and communicate it with colleagues, and the way we embrace risk as a core capability of our business.

Further training is 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 are integrated into the BAU.

Integration and accountability for risk in our processes

Risk is considered in the development of policies such as procurement, privacy, and 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 and sustained behaviours

Council's risk function is responsible for the design and operation of our risk management framework and are trusted risk advisors to Management. The risk team is central to helping embed risk into daily activities and to promoting staff engagement in ongoing risk discussions. The risk team role models risk behaviours and risk language and encourages openness and transparency in risk discussions, escalation and reporting. This approach helps to promote and sustain a common and shared understanding of risk throughout the Council.

Reporting

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 raise risk concerns in confidence where required:

- Our risk profiling sessions are forums for raising risk concerns and staff have the option to discuss risk in confidence as needed with the risk team.
- The Manager Corporate Services & Finance has a "dotted" reporting line to the Audit Panel on risk matters and can raise risk concerns directly.

Reporting requirements:

Under the *Local Government Act 1993*, Council is required to report to the Audit Panel on the development, implementation and effectiveness of its RMF and risk profile, including any significant business, compliance and/or emerging risks.

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.

Risk reporting is performed according to the needs of the recipients, but the content reflects Council's risk culture. Further detail on risk reporting and application of the RMF is provided in the Risk Procedures.

Definitions

Term	Definition
Consequence	The outcome of an event upon organisational or operational objectives. This can be either positive or negative and can be expressed either quantitatively (e.g., in financial terms) or qualitatively (e.g., being a loss, injury, disadvantage or gain).
Control	The measure to modify a risk. This can include a policy, procedure, practice, process, technology, technique, method, or device that modifies or regulates risk.
Current level of risk	The level risk at a point in time, based on the known level of control effectiveness, and rated against the risk rating matrix.
Event	An occurrence or something that has happened that has both a cause and a consequence. By comparison, a risk has not happened but *could* happen.
Internal audit	An independent, objective assurance and consulting activity that brings a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, controls, and governance processes.
Likelihood	The chance or probability of something happening. This can also be expressed quantitatively or qualitatively.
Near miss	An event without tangible consequences.
Operational risk	The risk of loss resulting from inadequacies or failures in people, processes, and systems. These are encountered in everyday operations, such as delivering services and promises to the community.
Project risk	Events that can stop a project or initiative from being a success, such as budget blowouts, delivery delays or failure to achieve the project objectives.
Risk	The effect of uncertainty on objectives.

	• An effect is a deviation from the expected which can be positive or negative. • Uncertainty is the level of unknown measured in terms of likelihood. • Organisational objectives (such as financial, health and safety, technology and environmental goals) can apply at different levels (such as organisation-wide, operational, project, product and process). • Risk is usually expressed in terms of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.
Risk appetite	The amount of risk that an organisation is prepared to accept or take on in the pursuit of objectives.
Risk culture	The behaviours, attitudes and awareness that determine how people think about and manage risk.