Enterprise Risk and Opportunity Management Framework

Monash City Council

Version 6, July 2024

Table of contents

1. Preface

Monash City Councils' mission is to "provide facilities and services, and advocates for the community, through the well-planned and balanced assessment of needs, for those who live, work and play in Monash. We listen to our community and research to ensure good decision making" (Council Plan 2021-24). This mission (and the associated objectives, priorities and measures) support the delivery of the Monash Community Vision (Imagine Monash in 2040) that "Monash is the most liveable city in Victoria".

The Enterprise Risk and Opportunity Management Policy and Enterprise Risk and Opportunity Management Framework (ER&OMF) is a key component of Council's governance arrangements. It is the structure upon which the risks, opportunities and other information that may impact the achievement of Council's goals and strategies are identified and managed. Through the ER&OMF, 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 the success of delivering Council's mission and the community's vision for Monash.

The ER&OMF is based upon the International Risk Management Standard (adopted 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 ER&OMF outlines the arrangements for designing, implementing, monitoring, reviewing and continually improving risk management across all Council activities.

This 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. Purpose

The key purpose of the ER&OMF is to assist Council achieve its goals and objectives in delivering programs and services as outlined in the Council Plan.

Council's approach to risk management is designed to:

- Support 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
- Create and protect value by targeting effort and resources to the areas of highest priority.

The application of the ER&OMF will assist with:

- Achieving the objectives of the Council Plan
- Protecting people, assets, finances and Council reputation
- Taking risks in accordance with approved policies and values
- Adopting risk treatments that are fit for purpose, cost effective and designed to reduce risk to a tolerable level

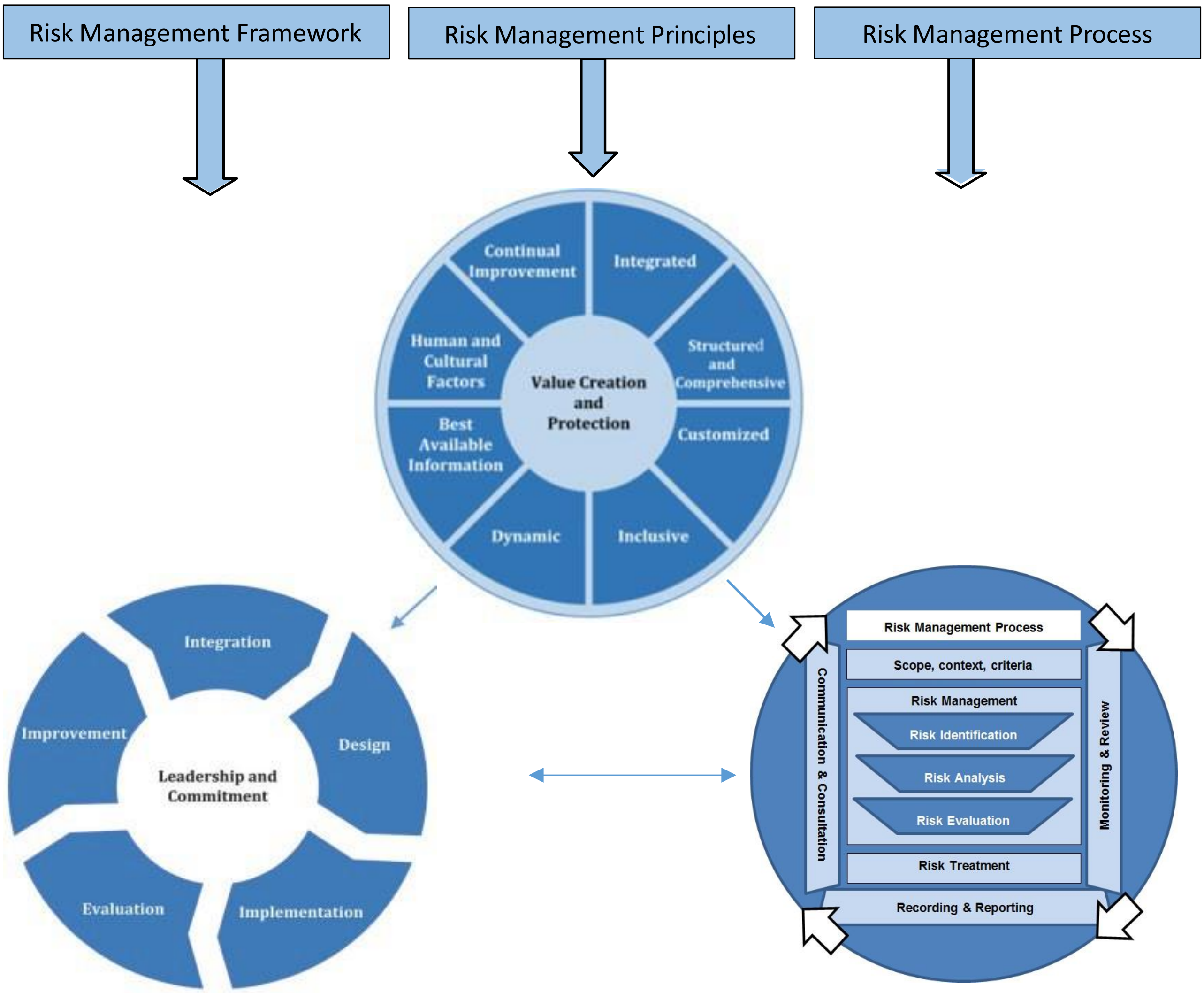
- Embedding a culture that promotes awareness and accountability for risk so it becomes a key part of decision making at Council.

3. Principles, components and procedures of the ER&OMF

Risk and opportunity is defined as ‘something happening that may have an impact on the achievement of objectives’. Risk and opportunity management describes the planned and systematic approach used to identify, evaluate and manage the whole range of business risks and opportunities facing the Monash City Council.

Councils’ approach to risk and opportunity management is underpinned by the principle that risk management is the responsibility of all: Councillors, executive, managers, coordinators, officers, contractors, volunteers etc.

Figure 1: Risk management proposition



This ER&OMF 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 the City of Monash, these being (and further explained in Appendix A):

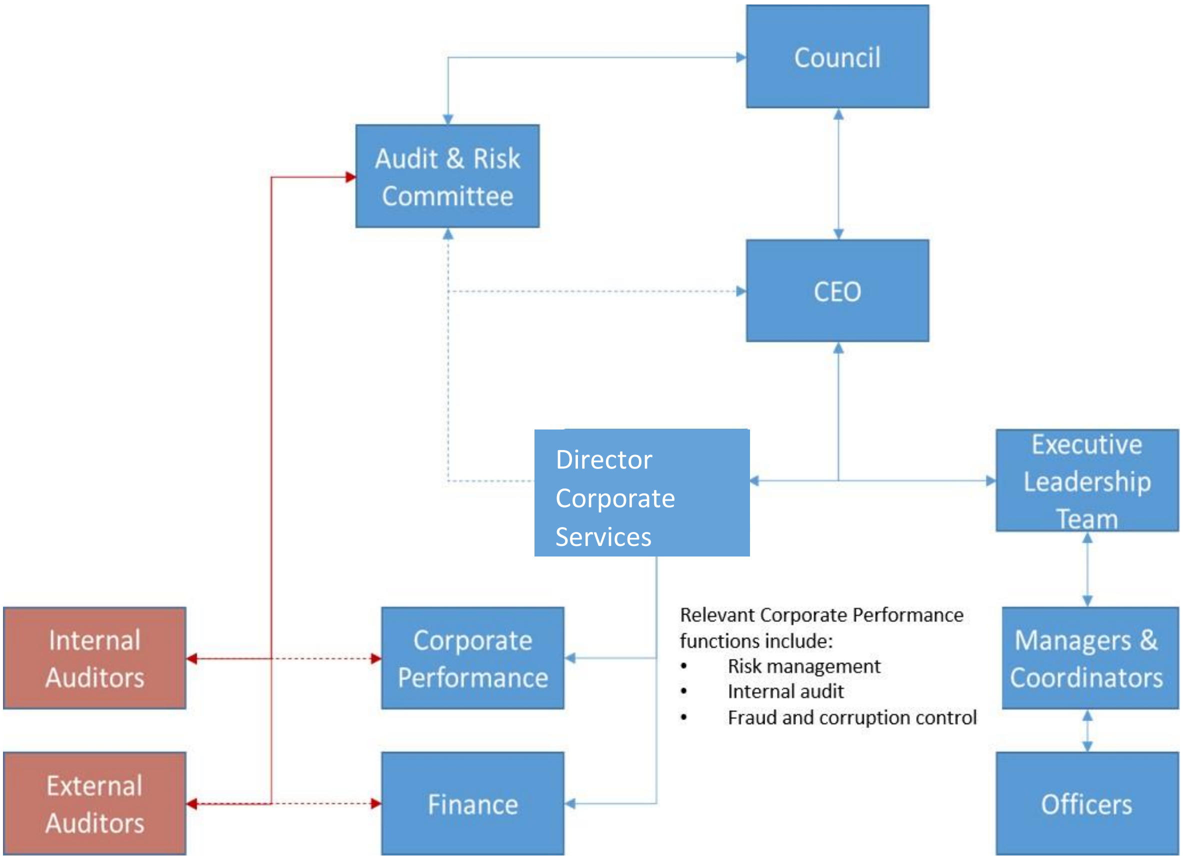
1. Creates value and protects assets
2. Is integrated into Council's daily activities
3. Is structured and comprehensive
4. Is customised to Council's internal and external context
5. Is inclusive of a range of perspectives from key stakeholders
6. Is dynamic and is responsive to organisational change
7. Is based on best available information
8. Takes human and cultural factors into consideration
9. Facilitates continual improvement through learning and experience.

4. 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.

It starts with the Councillors and cascades through management and all levels of staff. Oversight of risk is achieved through the Audit and Risk Committee, with independent assurance from the internal audit function.

Figure 2: High level overview of risk management governance structure



Relevant Corporate Performance functions include:
- Risk management
- Internal audit
- Fraud and corruption control

5. Risk Management Committee

Membership of the Risk Management Committee comprises of the Executive Leadership Team, Manager Corporate Performance and the Coordinator Business Assurance and Risk Management. The Committee meets on average every two months to:

- Review and update the Strategic Risk Register;
  - noting any changes to causes, consequences and controls
  - considering further mitigating strategies
  - considering changes to the Register due to emerging risks or effective control of existing risks
- Discuss new and emerging risks
- Identify if specialist risk management advice is required
- Review the Operational Risk Register;
  - reviewing the management of any Extreme or High Operational risks
  - review the effectiveness of 'organisational 'controls
- Review the ER&OMF
- Review risk management culture within the organisation.

6. Risk management function

Council's risk management function largely sits with the Coordinator Business Assurance and Risk Management (the Coordinator) who reports to, through the Manager Corporate Performance, to the Director of Corporate Services, and to the Executive Leadership Team.

The Coordinator is not primarily responsible for the management of risks but is responsible for supporting all business units in managing risks for which they have ownership. Key responsibilities include:

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

The Coordinator's role has no operational business line responsibilities and is fully independent. Key responsibilities are facilitating regular risk profiling, enterprise risk reporting and maintenance of the ER&OMF and risk register, working with Council's divisions to assist and advise on the application of the ER&OMF.

7. Roles, responsibilities and accountabilities

The roles and responsibilities for risk management at Council are specified in this policy, committee charters and individual position descriptions.

Figure 3: Roles and responsibilities for risk management

Personnel	Accountabilities and responsibilities
Council (Councillors)	• Oversight of risk management through policy setting at Council. • Oversight of the Audit and Risk Committee • Periodic review of organisation's strategic risks.
Chief Executive Officer	• Overall accountability for risk management. • Setting and role modelling 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 functions.
Audit and Risk Committee	• Independent review and oversight of Council's governance, risk management and control activities. • Oversight of the internal audit function.
Internal audit	• Risk assurance as to the effectiveness of the operation of controls that mitigate risks to the Council, Audit and Risk Committee and CEO through execution of the internal audit plan.
Monash Risk Management Committee (ELT)	• Accountable for approval, ownership and management of strategic risks. • Accountable for approval, ownership and management of operational risks in their respective areas of responsibility or as delegated by the CEO. • Role modelling the tone, culture, risk appetite and expectations for risk management and governance activities. • Accountable for the risk management performance of staff in their respective areas of responsibility.
Coordinator Business Assurance and Risk Management	• Leading the risk management function. • Developing and implementing an enterprise risk and opportunity management framework that is fit for purpose. • Risk reporting to the Audit and Risk Committee. • Supporting ELT and managers to manage their risks through: ○ Provision of risk management advice and guidance to staff. ○ Maintenance of the enterprise risk & opportunity management framework.
Managers and Coordinators	• Accountable for the management of risks in their respective areas of responsibility. • Accountable for risk assessments and completion of risk actions in their respective areas of responsibility.

8. Risk assurance

Three lines of defence

Council operates a ‘three lines of defence’ (3LOD) model to actively manage, monitor and oversee risk.

The first line of defence 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 team responsible for risk management.

The focus of the second line of defence is on managements testing of 1st line controls (independent of the operational unit) is ensuring first line controls are in place, properly designed, operating as intended and governance of controls is effective. As part of this assessment, controls are reviewed, and improvements recommended to operational units and overall trends reported to senior management.

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

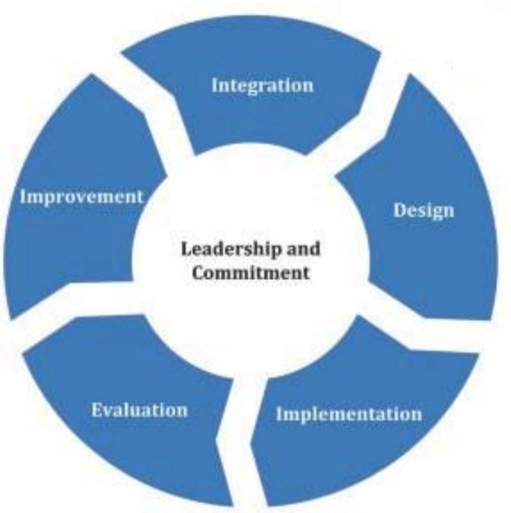
Assurance activity is guided by the internal audit plan. It is an efficient use of resources to integrate risk management into the internal audit plan. That is, the internal audit plan takes into consideration Council’s risk profile and targets assurance activities towards higher rated risks and/or matters 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.

Figure 4: Components of the ‘three lines of defence’ model

First Line of Defence	Second Line of Defence	Third Line of Defence
All management in the Monash City Council divisions: • Executive Office including People and Safety and Communications and Customer Experience • Community Services • Corporate Services • City Development • City Services	• Enterprise Risk Management • Financial Services • People and Culture • Legal Counsel • Strategic Procurement • Self-assessments against relevant Integrity Agency reports	• Internal Audit • External Audit Note that internal audit are separate to external audit whose role is to review the integrity of Council’s financial records.

9. Integration of risk into Council activities



Source ISO31000:2018

Leadership and commitment

Accountability for risk is promoted through the Councillors, CEO, Audit and Risk Committee and Executive Leadership Team and endorsed through the Enterprise Risk and Opportunity Management Policy and the ER&OMF. Further the risk appetite (to be adopted) demonstrates Council's commitments 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 ER&OMF.

As noted in roles and responsibilities section, leaders are accountable for setting the tone for risk across the organisation.

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 or can assist to prevent value destruction.

Figure 5: Examples of incorporating risk management into BAU activities

Key council activity	Example of where or how risk management is integrated
Strategic planning	Risks to the delivery of the Council Plan

Key council activity	Example of where or how risk management is integrated
Project development and service delivery oversight (both corporate centre and community initiatives) to agreed levels	Business case development Status monitoring and oversight Performance reporting
Internal audit plan	The internal audit 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
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 & 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

Design

This ER&OMF considers, amongst others, Council's role in the community, its obligations, objectives and business processes, to create framework that is tailored to suit Council's needs and operating environment (ensuring it is fit for purpose). As demonstrated in this document, the ER&OMF has assigned roles accountabilities and resources for risk management and the channels for risk consultation are described in the separate Risk Procedures Manual.

Implementation

The risk strategy and related timeline, part of Council's operational risk workplan, 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.

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 through performance management managed by People and Safety) in accordance with Council's risk appetite.

Improvement

The ER&OMF 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 ER&OMF components outlined in this document.

10. Risk appetite

Risk appetite links risk management process to Council's strategy and supports Council in making informed decisions.

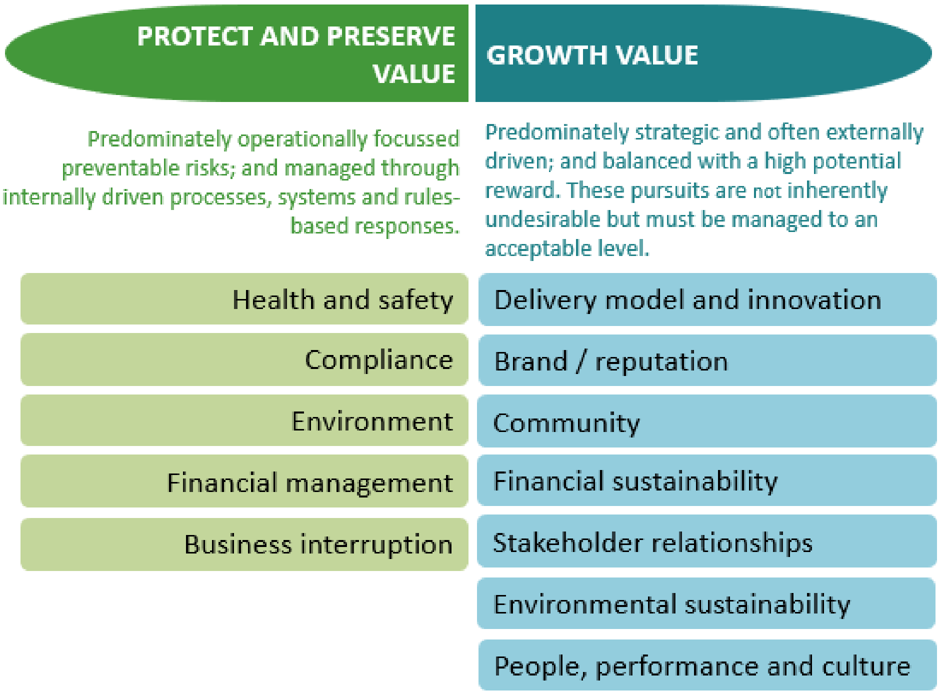
A clearly articulated risk appetite, combined with the Council Risk Profile and appropriate risk indicators establishes the basis for Council and the Executive to assess whether the organisation is operating within acceptable risk parameters.

It provides leaders with the context to communicate and translate - through policies, procedures and delegations - what level of risk taking is acceptable in day-to-day organisational activities and decision making.

Monash City Council recognises that the identification and management of risk is central to delivering on our purpose and achieving our strategic and operational objectives.

A number of categories have been developed that articulate Council's appetite levels, these are structured by the business value they present.

- Our appetite for preserving and protecting business value, measured after applying controls, processes and practices to effectively manage these risks, is cautious. They are predominately operationally focussed preventable risks; and managed through internally driven processes, systems and rules-based responses.
- However, in pursuing strategic initiatives that grow business value, we adopt a balanced risk appetite commensurate with the strategic choices we have made and we are committed to managing those risks in a considered and effective way. They are predominately strategic and often externally driven; and balanced with a high potential reward. These pursuits are not inherently undesirable but must be managed to an acceptable level.



PROTECT AND PRESERVE VALUE	GROWTH VALUE
Predominately operationally focussed preventable risks; and managed through internally driven processes, systems and rules-based responses.	Predominately strategic and often externally driven; and balanced with a high potential reward. These pursuits are not inherently undesirable but must be managed to an acceptable level.
Health and safety	Delivery model and innovation
Compliance	Brand / reputation
Environment	Community
Financial management	Financial sustainability
Business interruption	Stakeholder relationships
	Environmental sustainability
	People, performance and culture

Risk appetite levels

Risk appetite level	Description
Zero risk appetite	The organisation will avoid the risk and uncertainty. In such cases, they will choose to stop the activities to simply avoid the risks. For example: • We won't accept any actions or behaviours that willingly contravene the Code of Conduct, Occupational Health and Safety policies and procedures or other relevant policies. • We won't tolerate any practices that knowingly compromise staff wellbeing, workplace or community safety including discrimination, harassment or bullying.
Cautious risk appetite	The organisation will accept as little risk as possible and adopts a cautious approach to taking risk. It is unwilling to accept avoidable risks, which, if accepted, could have a significant negative impact on the business. Council will undertake all reasonable measures to reduce, limit or avoid such risk. For example: • We will establish controls and processes that could prevent cybersecurity threats or significant threats arising from external malicious attacks. • We will set up policies, procedures guidelines to prevent material breaches of legislations or legal obligations. • We will put up systems, processes and controls which adequately protect Council from fraudulent or corrupt financial transactions.
Balanced risk appetite	The organisation is willing to accept risks to a certain degree in return for a level of reward or value for money. In these cases, Council will have a balanced and informed approach to risk taking, and will be accepting that incidents will occur however, the impact and frequency is such that additional investment in controls is not justified. For example:

Risk appetite level	Description
	• We are open to business innovation by exploring the way we work to provide improved services to our communities, i.e. sharing control with other stakeholders in delivery service whilst retaining accountability for outcome. • We are open to exploring new strategies that grow and diversify our income portfolio but carry some level of risk. • We are open to investing in new technologies and approaches to achieve our objectives regarding environmental sustainability. We will recognise and where appropriate accept a balanced and manageable level of risk regarding the financial and service delivery impacts of these approaches
Aggressive risk appetite	The organisation is willing to take significant amount of risk in pursuing strategies in return for the highest rewards. It will apply a responsible approach to taking an aggressive risk for an increased benefit or to achieve Monash's strategy, and will encourage optimisation of the risk and reward equation. For example; we are open to undertaking entrepreneurial investment in a commercial enterprise. While this can magnify returns, it also significantly increases the financial risks in case of unfavourable outcomes. *Note: Generally, it is very rare to see local governments to have an aggressive risk appetite. The nature of local government's roles and responsibilities including managing public funds and public safety, typically encourages a more balanced/cautious approach, prioritising the stability and well-being of the community.*

Growth value sub-category risk with tolerance levels and metrics

Risk category and description	Appetite level	Risk tolerance (qualitative metrics)	Risk tolerance (quantitative metrics)
Brand (reputation) Risks associated with actions and activities that are misaligned with Monash's values and our brand. Risks associated with our brand being prominent in the public domain, where it is relevant to our purpose and strategic objectives.	Cautious	**Tolerance statement:** We have a very low tolerance for risks associated with actions and activities that undermine our reputation and negatively impact on our brand. The use of our brand must be consistent with and guided by council's values and strategic objectives, and undertaken in compliance with all applicable legislation, rules, and policies. **Our approach:** We apply a cautious risk tolerance to communication and use of our brand which must be consistent with and guided	• Evaluation of media posts negative to Council brand. • CSS results where performance satisfaction is 20% below importance score. • Social media posts (% of support or no support to posts). • Complaints register.

Risk category and description	Appetite level	Risk tolerance (qualitative metrics)	Risk tolerance (quantitative metrics)
		by organisational values, and undertaken in compliance with all applicable legislation, rules and policies.	
Community[1] The end beneficiaries of the services and activities we provide. Risks associated with strategic choices when viewed from the perspective of our communities.	Cautious	**Tolerance statement:** We have a cautious tolerance for negative reaction associated with strategic choices when viewed from the perspective of our communities. **Our approach:** Rigorous due diligence, including community engagement, that will lead to evidence-based decisions and strong change management approach is essential. We are committed to engaging our community in terms of making strategic decisions.	• Annual Customer Satisfaction Survey results where performance satisfaction is 20% below importance score. • Adherence with community engagement framework policy. • Influence of engagement findings in the development of strategies and plans. • Detailed community impact assessment, including community profiling (and forecast) for subject. • Assessment of compliance with council reporting (council plan, human rights, social, financial, environmental).
Stakeholder Relationships[2] The partners, collaborators, private and government entities we work with to achieve our strategic and operational objectives.	Balanced	**Tolerance statement:** We recognise the risks associated with setting and balancing stakeholder expectations in relationships that are critical to successfully delivering on our objectives. We have a balanced tolerance for risks associated with stakeholder management and we are open to explore the new/innovative ways of engaging stakeholders to deliver service to the community.	• Performance reporting based on contract levels of service (maximise benefit). • Number of mapped relationships and governance structures in place. • Feedback on stakeholder performance as part of due diligence/research. • Council performance KPIs (Key Performance Indicators) in contracts. • Quality of internal audits. • Level of service standards of stakeholders.

[1] *Community being the end beneficiaries of the services and activities we provide.*

[2] *Stakeholders being the partners, collaborators, private and government entities we work with to achieve our strategic and operational objectives.*

Risk category and description	Appetite level	Risk tolerance (qualitative metrics)	Risk tolerance (quantitative metrics)
		Our approach: We manage these risks to an acceptable level through strong controls including governance arrangements and contract management.	
Delivery Model and Business Innovation The ways and approaches of how Council delivers a range of services, events and facilities to the community.	Balanced	**Tolerance statement:** We recognise the risks associated with adopting new and innovated approaches. This includes new/innovative ways of engaging stakeholders to deliver service to the community, for example, sharing control with other stakeholders in delivery service whilst retaining accountability for outcome. We adopt a balance risk tolerance to our delivery model. We are open to business innovation by exploring the way we work to provide improved services to our communities. **Our approach:** When we explore modern options, we recognise the risks inherent in our environment and our capacity. We are committed to make evidence-based decisions following undertaking the due diligence.	• Review and reporting of delivery models (service planning).
Financial Sustainability Consideration and management of revenue and expenditure from a long-term perspective	Balanced	**Tolerance statement:** We recognise the risks associated with pursuing strategies that achieve long term financial sustainability including: • New strategies to grow and diversify our income portfolio. • More cost-effective approaches to	• Assessment against Financial Plan and financial modelling part of due diligence. • LGPRF financial and performance indictors. • Financial performance to Budget. • Budget variations including assessment of net cost impact to council.

Risk category and description	Appetite level	Risk tolerance (qualitative metrics)	Risk tolerance (quantitative metrics)
		service delivery that do not compromise community outcomes. We adopt a balanced risk tolerance to ensure financial sustainability in the long term. **Our approach:** We identify the full range of financial and non-financial risks associated with new initiatives that secure and grow existing funding and diversify income streams.	• Budget targets (grants, income, fees, and charges) and measure to forecasting. • Ongoing assessment of whole of life cost impact to council/community. • Impact of outcome of legislation or initiatives introduced by other levels of government (cost/benefit analysis).
People & Inclusive and Diverse Culture People's skills and capabilities as well as council's overall performance and culture.	Balanced	**Tolerance statement:** We adopt a balanced tolerance for risks associated with adopting the strategies necessary to enhance the skills and capabilities of our people in a growing environment whilst also setting commensurate standards of performance and accountability for our staff. We adopt a balanced tolerance for risks associated with creating a culture that removes barriers to engagement, participation, inclusion, and diversity. **Our approach:** We support and enhance the skills, capabilities of our staff to maximise delivery through adopting contemporary approaches. We focus on extensive and transparent consultation and communication within the organisation, and more	• Labour profiling and capability assessment • Compliance with existing policies (eg officer and councillor code of conduct) • Recruitment compliance with policy/processes. • Protection and compliance relating to public interest disclosures • Workforce planning including succession planning • Regional collaboration opportunities explored with other councils • Training program review offered to staff (enhancement, retention, capability) assessment and officer feedback result.

Risk category and description	Appetite level	Risk tolerance (qualitative metrics)	Risk tolerance (quantitative metrics)
		broadly with our large and diverse stakeholder cohort.	
Environmental sustainability The sustainability considerations in the decisions that have a potential impact on the environment.	*Balanced*	**Tolerance statement:** We recognise that our role in environmental stewardship and contribution to sustainability as an environmentally responsible organisation is a key strategic priority. We have a balanced risk tolerance, recognising and balancing risks associated with our financial capacity to deliver and the inherent tension between our service delivery obligations and their associated environmental impact. **Our approach**: We accept some cost impacts in the selection of products, services that have a significant positive impact on the environment. In pursuit of our activities and projects, we proactively consider changes to procedures and practices to accommodate improved environmental outcomes.	• Performance to targets set, and/or measure of impact of decision to targets. • Review of customer/community understanding of issues and initiatives relating to environment impact. • Development of EIS (Environment Impact Statement) part of decision making process for major projects/service decisions.

Protect and preserve value category risks with tolerance levels and metrics

Risk category and description	Appetite level	Risk tolerance (qualitive metrics)	Risk tolerance (quantitative metrics)
Financial Management Day-to-day financial activities associated with delivering a wide range of services, programs and capital projects.	*Cautious*	**Tolerance statement:** We recognise the financial risks involved in delivering a wide range of services, activities and capital projects. We have a low tolerance for inefficient	• Any cost variation larger than 10% requires corporate /council review. • Financial sustainability indicators remain in green zone.

Risk category and description	Appetite level	Risk tolerance (qualitive metrics)	Risk tolerance (quantitative metrics)
		and ineffective use of financial resources. **Our approach:** We are cautious for variation in financial performance.	- Fraud and corruption incidences
Health & Safety, HR A wide range of activities associated with staff and public health and wellbeing	***Zero***	**Tolerance statement:** We recognise that our workforce is exposed to various hazards due to the many inherently high-risk activities that Council undertakes in delivering services and programs to the community. We have zero risk tolerance for actions that deviate from established procedures and practices or otherwise endanger our people's health, safety, and wellbeing. **Our approach:** We are committed to providing a safe workplace for our workforce, contractors and visitors. We manage these risks to the lowest practicable level through a mature and robust health and safety management system and specific processes and practices to support safeguarding our employees, contractors and wide community. In addition, by virtue of the nature of our activities, we have a high level of contact with, and commensurate duty of care towards children and young people.	- Reporting on reportable incidents and near misses - Number of reported OHS breaches - Number of reported fraud and corruption incidences - Reporting on leave accruals - Compliance to HR policies and processes (recruitment, leave, OHS etc)

Risk category and description	Appetite level	Risk tolerance (qualitive metrics)	Risk tolerance (quantitative metrics)
Compliance Governance process and meeting legislated and regulatory requirements.	***Cautious***	**Tolerance statement:** We recognise the risks associated with the multitude of compliance obligations that arise from the many and varied activities undertaken by Council. We have a low tolerance for significant breaches of regulatory obligations and associated Council policies. **Our approach:** We manage compliance risks through ensuring a full understanding of our legislative obligations and translating those obligations to effective policies, procedures and guidelines.	• Legislative compliance framework reporting (annual attestations). • Compliance and tracking of performance from internal and external audits • Other statutory service reporting (eg stat planning, aged care, immunisation etc)
Environment Environmental impacts arising from normal business activities.	***Cautious***	**Tolerance statement:** We recognise risks associated with effectively managing the environmental impact of Council's activities. We have a low risk tolerance for activities and projects that result in detrimental impacts on the environment. **Our approach**: We seek to minimise those impacts to the greatest extent possible whilst maintaining delivery of services in a cost-effective manner.	• Impact and delivery to environment targets set and endorsed by Council • ESG reporting • EPA fines • EPA and reporting offenses directing due to Council breaches.
Business Interruption Disruption to Council activities that impacts our capacity to deliver services to our communities.	***Cautious***	**Tolerance statement:** We recognise risks associated with a disruption to Council activities resulting in a material impact upon our capacity to deliver	• Business Continuity Plans for each department in place and updated. • Adherence and impact on reportable levels of services due to business interruption events.

Risk category and description	Appetite level	Risk tolerance (qualitive metrics)	Risk tolerance (quantitative metrics)
		services to our communities. We have a low tolerance for failing to recognise risks that could cause interruption to service delivery. **Our approach:** We are committed to deliver our critical services to serve the community by having appropriate business continuity plans to respond to a disruption and ensure timely recovery and continuity of critical business.	

11. 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.

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	Reputation & stakeholder relationships Financial Health & safety, HR Compliance Environment & business interruption/IT	Community, State Government and media outrage, key relationships broken down Financial impact >$5mil Fatality Regulatory investigation, legal action, fines and penalties imposed Uncontrolled spread of toxic pollutants. Building destroyed and BCP invoked. System downtime expected for >2 weeks and DR invoked		High	High	Extreme	Extreme	Extreme
MAJOR	Reputation & stakeholder relationships Financial Health & safety, HR Compliance Environment & business interruption/IT	Widespread community concern , adverse media coverage, key relationships severely damaged Financial impact $1mil - $5mil Injury or illness requires emergency response, hospitalisation Reportable breaches and regulatory investigation at Council level Spread of toxic pollutants is widespread. Building severely damaged and BCP invoked. Systems downtime is widespread and DR invoked		Moderate	High	High	High	Extreme
MODERATE	Reputation & stakeholder relationships Financial Health & safety, HR Compliance Environment & business interruption/IT	Well publicised community concern, limited media coverage and some key relationships strained Financial impact $250k - $1mil 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 and systems interruption is localised and BCP/DR is not invoked		Moderate	Moderate	Moderate	High	High
MINOR	Reputation & stakeholder relationships Financial Health & safety, HR Compliance Environment & business interruption/IT	Community concern is voiced locally, key relationships not impaired Financial impact $50 - $250k 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 or building damage and systems interruption is limited and BCP/DR is not invoked		Low	Moderate	Moderate	Moderate	High
IN-SIGNIFICANT	Reputation & stakeholder relationships Financial Health & safety, HR Compliance Environment & business interruption/IT	Negligible community concern and impact to public image Financial impact <$50k 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 and system interruption is negligible		Low	Low	Low	Moderate	Moderate

12. 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.
Moderate	Risk is on the tolerance boundary. Escalate to management.	Treatment plan to commence within 4 weeks with regular oversight from senior management.
Low	Risk is within tolerance boundaries but outside of the preferred operating range.	Treatment options and oversight plan to be developed with management.

13. Risk profiles

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.

Council's risk team coordinates strategic and operational risk profiling activities on a 6 monthly basis. Projects outside of this undertake risk assessments on an as-needs basis.

Council's risk profile is comprised of:

Strategic risks

Strategic risks are risks to the delivery of Council objectives, mission and Council's Strategic Plan.

Operational risks

Operational risks will be encountered in everyday business activities. i.e service delivery and project management.

Emerging risks

Emerging risks are not currently on the risk register but require periodic monitoring and review.

14. Risk register

The Strategic Risk Profile and Operational Risk Profiles are reviewed annually and stored in the corporate reporting software. All Managers and Executive Team, have access to the systems and reports of these quarterly. The software is used to record risks, record and monitor treatment activities, assign responsibility for treatments, monitor treatments, identify controls, record control effectiveness assessments and generate risk reporting.

Key fields in the risk register are:

1. Risk – What could happen and how serious could it be?
2. Causes – Why/how could the risk event happen?
3. Controls in place - What is in place to mitigate/manage the risk?
4. Control effectiveness rating – When was the control last reviewed and how effective was it at managing the risk?
5. Current risk rating – Given the effectiveness of risk controls, how significant is the risk now?
6. Treatment - What more needs to be done to manage the risk to within tolerance levels? Depending on the materiality of the current risk exposure, there are several risk treatment options available:

Refer to Enterprise Risk and Opportunity Management Procedures Manual for further detail on the risk profile review process.

15. Controls

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).

It is managements expectation that controls are:

- Documented in a risk assessment
- Documented in the CAMMS Risk module
- Evaluated for its effectiveness
- Assigned to an owner.

Control effectiveness

Controls are effective when the control design appropriately addresses the risk, and the control works as expected, every time.

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.

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 effectiveness ratings

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.

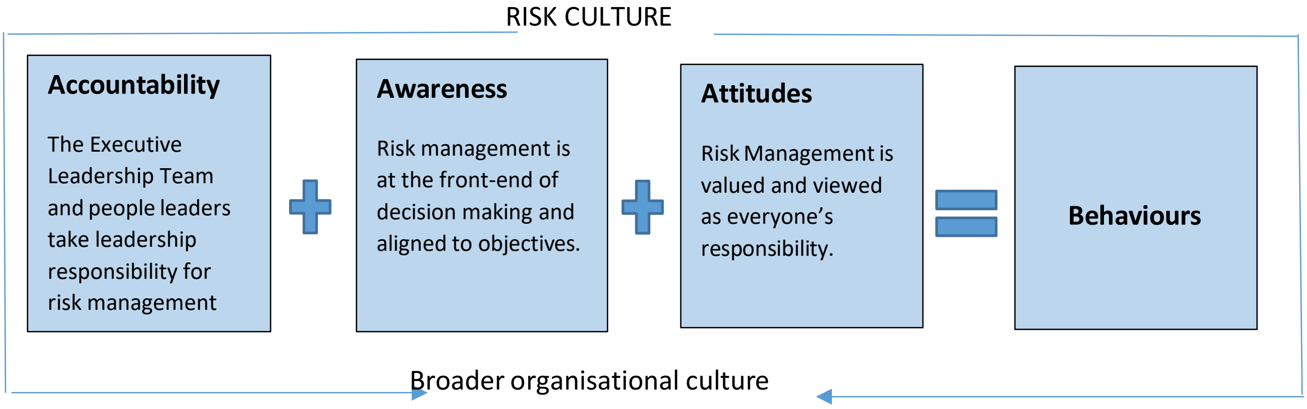
16. Risk treatment options

Decision	**Indicators**
Avoid the risk	Decide not to proceed with the policy, program or activity or choose an alternate means of action as it is outside our tolerance level.
Accept the risk	Council has made a conscious decision not to treat the risk, because: a) The cost of controlling the risk outweighs the benefits (reduced likelihood and consequence) of controlling the risk, or b) There are no effective controls available to reduce or eliminate the likelihood or consequence of 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 consequences if the risk event were to occur.

17. 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 the City of Monash.



RISK CULTURE

Accountability

The Executive Leadership Team and people leaders take leadership responsibility for risk management

Awareness

Risk management is at the front-end of decision making and aligned to objectives.

Attitudes

Risk Management is valued and viewed as everyone's responsibility.

Behaviours

Broader organisational culture

Source: Victoria Government Risk Management Framework Practice Notes – Risk Culture

Risk culture takes the inherent values and beliefs of individuals and translates this through the ER&OMF 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.

Risk culture at the City of Monash is evident through our:

- Codes of conduct
- Adherence to our delegated authorities
- Values
- 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.

18. Risk 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.

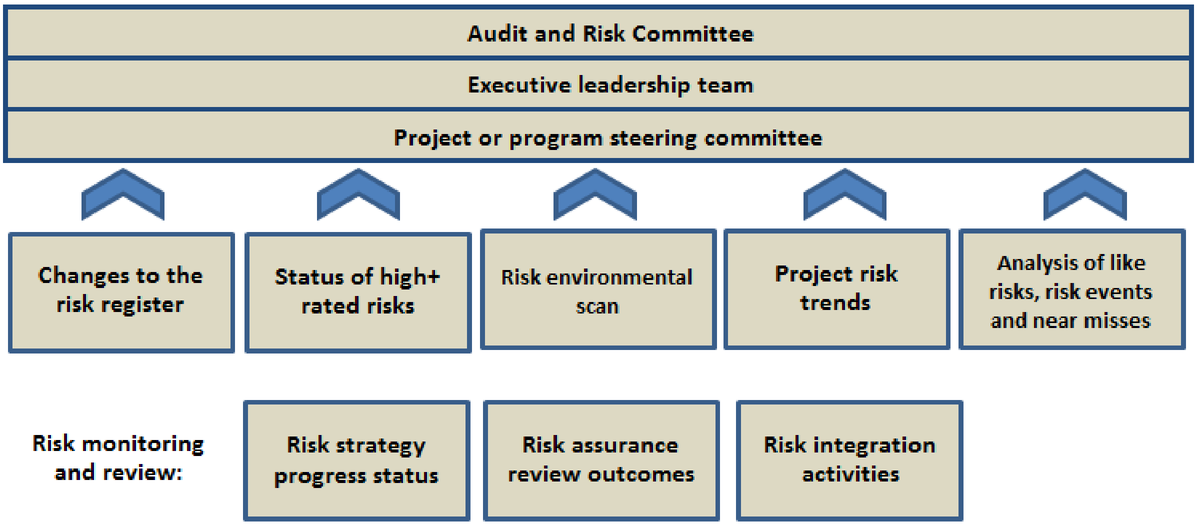
Opportunities to discuss risk matters in an open and transparent environment are available during risk profiling sessions.

Reporting requirements

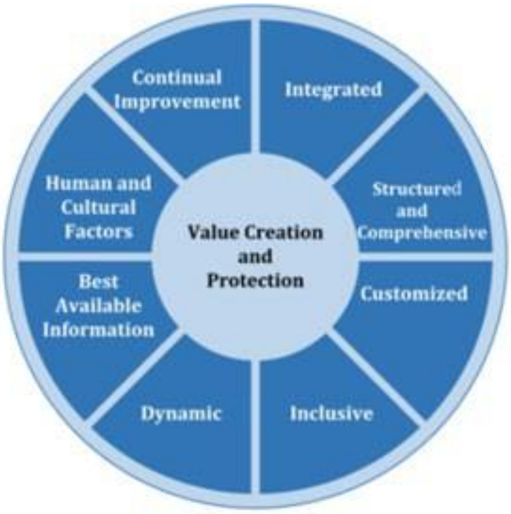
Under the Local Government Performance Reporting Framework, there is an expectation that Council generates a six-monthly report of strategic risks to Council's operations, including their likelihood and consequences of occurring and risk minimisation strategies.

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.

Risk reporting is performed according to the needs of the recipients, but the content is a reflection of Council's risk culture. Our reports are generally exception based and can include any of the following:


Audit and Risk Committee
Executive leadership team
Project or program steering committee
Changes to the risk register
Status of high+ rated risks
Risk environmental scan
Project risk trends
Analysis of like risks, risk events and near misses
Risk monitoring and review:
Risk strategy progress status
Risk assurance review outcomes
Risk integration activities

Appendix A: Reconciliation; principles of the risk management framework


Continual Improvement
Integrated
Human and Cultural Factors
Value Creation and Protection
Structured and Comprehensive
Best Available Information
Customized
Dynamic
Inclusive

Source ISO31000:2018

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

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 ERMF.
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.