



RISK MANAGEMENT POLICY

Responsible Officer: Health Safety and Risk Officer	Adoption Date:	September 2014
	Approved By:	Council
Authorising Officer: Manager People and Culture	Review Date:	October 2017
	Policy Type	Major Council Policy

INTRODUCTION

Risk management is about identifying potential variations from Council objectives and managing these to maximise opportunity, minimise loss and improve decisions and outcomes.

CONTEXT

A key strategic objective of Council is to ensure that business operations are compliant. In this regard the *Local Government Act 1989* requires Council to develop and maintain adequate internal control systems. An effective risk management framework is a critical element of such systems. The International Standard ISO 31000:2009 Risk Management – Principles and Guidelines, the Enterprise Risk Management – Integrated Framework (2004) Committee of Sponsoring Organisations of the Treadway Commission (COSO) and other related good practice guides identify the key elements of an effective risk management framework.

Set out below is a diagram illustrating how the risk management process interacts with other key risk management documents.



SCOPE

This policy applies to all activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets.

Risk management will be recognised and practised by all Councillors, staff, service providers, contractors and volunteers including those involved with any affiliated entity, program or initiative.

Risk management will be applied at all levels of the organisation, in Council-level activities such as strategic planning and resource allocation, concerning business unit activities such as communications and marketing and human resources, through to business processes such as service delivery and new customer credit review. It will also be applied to special projects and new initiatives.

Generic sources of risk include:

- Business risks associated with achieving strategic objectives;
- Occupational health and safety risks;
- Natural events;
- Technology and technical issues;
- Management activities and controls; and
- Commercial and legal relationships with stakeholders.

PURPOSE

The purpose of this policy is to provide guidance for Council's enterprise risk management framework and processes. It defines key principles, provides objectives, identifies the supporting framework and tools, and summarises responsibilities for risk management.

POLICY

DEFINITION OF RISK

The International Standard ISO 31000:2009 Risk Management – Principles and Guidelines defines risk as:

'The chance of something happening that will have an impact on objectives. A risk is often specified in terms of an event or circumstance and the consequences that may flow from it. Risk is measured in terms of a combination of the consequences of an event and their likelihood.'

Managing risk includes identifying and taking opportunities to improve performance as well as taking action to avoid or reduce the chances of something going wrong.

COMMITMENT

This policy mandates the formal, systematic, integrated, structured and proactive management of risks across Council. Effective management of risk is vital to the continued growth and success of the organisation and will be conducted in line with the principles outlined in this policy.

Council recognises risk is inherent in all its activities. Management of risk is good business practice. It creates value; and, is often a mandatory legal requirement. Effective risk management will improve decision-making and planning and better identify opportunities and threats, maximising value from assets, projects and business opportunities; and assisting innovation.

Council is committed to funding prudent risk management, either via the business and budget planning process, or by reprioritising resource applications when uncertainty requires.

Clear roles and responsibilities are defined in this policy and associated procedures. Council will ensure that officers with key risk management roles and responsibilities are provided with the necessary training and authority. In addition, all staff will receive training to enable them to participate in risk management activities.

Council commits to effective engagement of stakeholders in its risk management processes.

COUNCIL'S RISK APPETITE

In conducting appropriate oversight, management must deal with a fundamental question: How much risk is acceptable in pursuing these objectives? This question is dealt with in the notion of Council's 'risk appetite'.

Risk management is not isolated from strategy, planning, or day-to-day decision making. Nor is it wholly about compliance. Risk management is part of Council's culture, just as making decisions to attain objectives is part of the culture. To fully embed risk management in Council, decision makers must know how much risk is acceptable as they consider ways of accomplishing objectives. They must consider risk appetite at the same time as deciding which goals or operational tactics to pursue. Risk appetite also guides resource allocation. Management allocates resources among business units and initiatives with consideration of Council's risk appetite and plans for achievement of objectives. Management must also consider risk appetite as it aligns its organisation, people, and processes, and designs infrastructure necessary to effectively respond to and monitor risks.

Risk Appetite Statement

Council operates within a low overall risk range. Council's lowest risk appetite relates to employee and public health and safety, environmental responsibilities, financial sustainability, delivery of essential services, organisational reputation and compliance objectives, with a marginally higher risk appetite towards its strategic, reporting, and operations objectives. This means that reducing to reasonably practicable levels the risks related to our work environment, achievement of public safety and environmental goals, operating within appropriate prudential limits, delivering essential services, and meeting our legal obligations will take priority over other business objectives.

Council has some appetite for risks that improve levels of service to the community, improve efficiency, reduce costs or generate additional income, so long as the tangible benefits from treating the risks are higher than the most cost-effective treatment costs, and there are no higher net benefit opportunities within Council's risk capacity.

RISK MANAGEMENT OBJECTIVES

The objectives of Council's risk management approach include:

1. **Achieving Council objectives** - within the context of the 2030 Community Vision, the Council Plan establishes strategic objectives, selects strategy, and sets aligned objectives. The enterprise risk management framework is geared to achieving those objectives, which are either:
 - Strategic – high-level goals, aligned with and supporting the vision;
 - Operational – effective and efficient use of its resources;
 - Reporting – reliability of reporting; or
 - Compliance – compliance with applicable laws and regulations.
2. **Maximising value for money** - by:
 - Gaining value from pro-actively managing uncertainty and variability;
 - Effectively allocating and using resources. Benefits in economy and efficiency can be achieved in the targeting of resources, protection of assets and avoidance of costly mistakes; and
 - Improving incident management and reducing loss and the cost of risk, including commercial insurance premiums.
3. **Enhancing governance** – by:
 - Improving compliance with relevant legislation;
 - Facilitating enhanced disclosure to executive and council officers through raising awareness of potential risks, and in demonstrating appropriate due diligence;
 - Improving capability to demonstrate that objectives are achievable within a tolerable level of residual risk to Council, the executive, auditors and insurance providers; and
 - Providing some protection for officers in the event of adverse events through reduced severity of outcomes and demonstration of appropriate due diligence by those accountable.

PRINCIPLES

Council will implement its approach to risk management in line with the principles identified in the International Standard ISO 31000:2009 Risk Management – Principles and Guidelines. The application of Council's approach to risk management will:

1. **Create and protect value** – by contributing to the demonstrable achievement of objectives and improvement of performance in, for example, health, safety, security, legal compliance, public acceptance, and environmental protection, service quality, and project management, efficiency in operations, governance and reputation. Specific measurable performance goals, measures and targets that demonstrate the achievement of objectives and the improvement of business and individual performance will be identified. All significant internal and external risks linked to objectives will be identified, assessed, treated and reported.
2. **Form an integral part of all processes** – such that it is not a stand-alone activity that is separate from Council's main activities and processes. It will form part of management responsibilities and an integral part of all processes, including strategic

planning and all project and change management processes. It will be tailored and embedded in culture, practices and processes, especially in policy development, service delivery and strategic planning, in a way that it is adequate, relevant, effective and efficient.

3. **Be an essential part of decision making** – by helping decision makers to make informed choices, prioritise actions and distinguish among alternative courses of action. Risks will be managed at the most appropriate level of management. The Risk Management Framework will include a defined risk stratification process, with a mechanism for elevating extreme or high level risks identified at the lower levels of the hierarchy, and delegating moderate risks identified at the higher levels of the hierarchy.
4. **Explicitly address uncertainty** – by ensuring that decision making at all levels involves explicit consideration of positive and negative effects of uncertainty on objectives based on best available information.
5. **Be systematic, structured and timely** – thereby contributing to efficiency and to consistent, comparable and reliable results. There will be communication and consultation plans, and reporting and escalation mechanisms in place to support and encourage individual accountability for risk, and timely and adequate reporting of risk.
6. **Be based on best available information** – including information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgement. In addition, decision makers will inform themselves of, and take into account, any limitations of data or modelling used or the possibility of divergence among experts. Appropriate mechanisms will be used to provide Council and CMT with consistent, comparable, accurate, timely and reliable results on performance against its strategy and objectives, the underlying causes of any performance variance and any changes in the internal and external environments or risk factors which would cause them to consider altering strategy and objectives.
7. **Be context aware** – by ensuring that risk management fits the external and internal context and risk profile of the strategic objective, process, project or task under consideration.
8. **Recognise human and cultural factors** - by recognising the capabilities, perceptions and intentions of individuals both external and internal to Council that can facilitate or hinder achievement of objectives.
9. **Be transparent and inclusive** – including appropriate and timely involvement of stakeholders and, in particular, decision makers at all levels, thereby ensuring that risk management remains relevant and up-to-date. Involvement will allow stakeholders to be properly represented and to have their views taken into account in determining risk criteria.
10. **Be dynamic, iterative and responsive to changes** – such as external and internal events, context and knowledge changes. Continual monitoring and review of new and emerging will support appropriate responses.

11. **Facilitate continual improvement** – through the development and implementation of strategies to improve risk management. A periodic review will determine whether the risk management framework, policy and plan are still appropriate and relevant to the external and internal context of the organisation. The output of this process is the Risk Management Strategy.

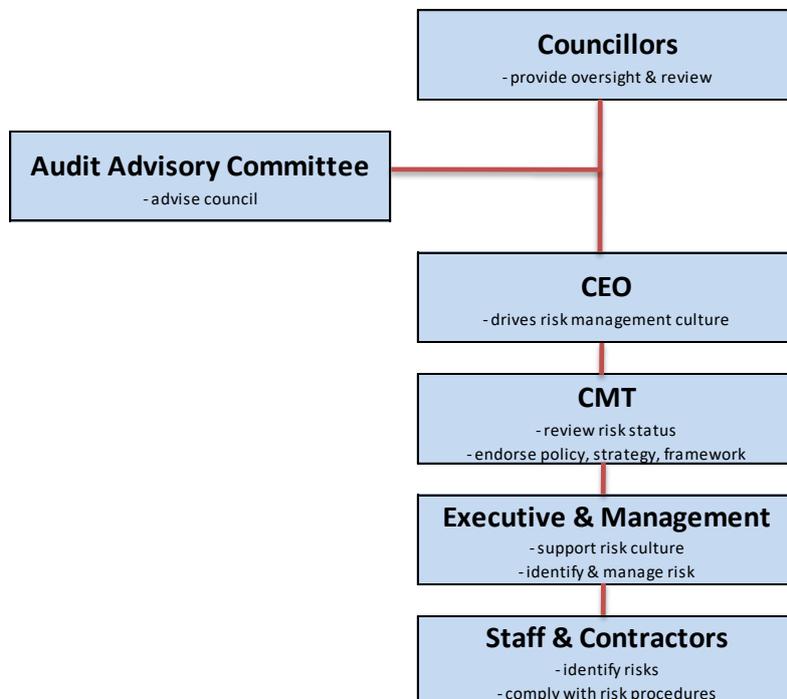
12. **Support achievement of Best Value principles** – which require, among other matters, that:

- All services provided by Council must meet the quality and costs standards required by the Act,
- Council must achieve continuous improvement in the provision of services for its community; and
- Council must be able to demonstrate and report to the community that it effectively applies Best Value principles.

RESPONSIBILITIES

Capability for effective risk management is dependent upon having an appropriate risk governance structure and well-defined roles and responsibilities. It is imperative that everyone is aware of their individual and collective risk management responsibilities and that people to behave in a way that is consistent with the approved policy, framework and process.

Risk management is not the sole responsibility of one individual but rather occurs and is supported at all levels of Council as illustrated below.



KEY PERFORMANCE INDICATORS

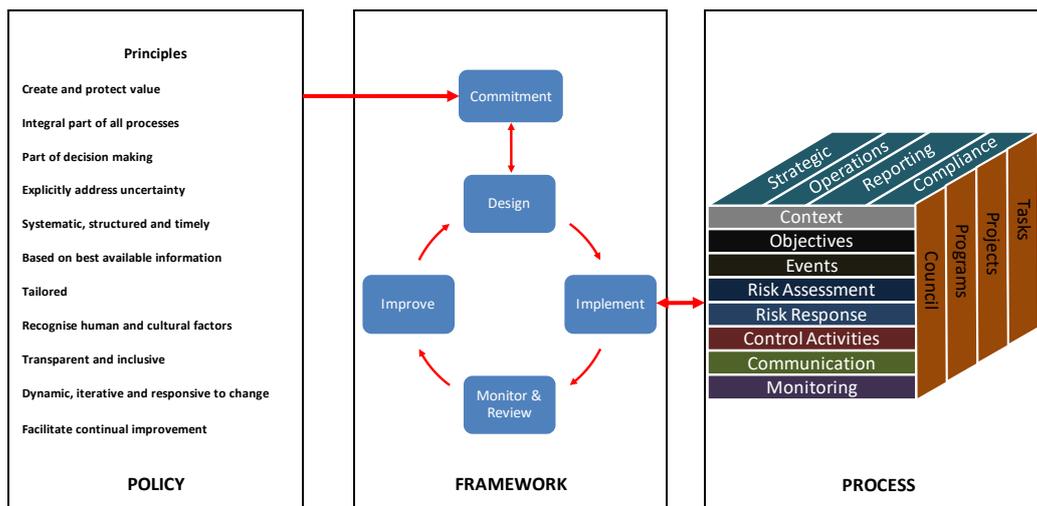
Key performance indicators will be used to monitor the effectiveness of, adoption of, and adherence to the risk management policy framework and processes. A mix of lead and lag indicators will be used, including:

1. Business assurance audit scores relating to conformance to the requirements of the risk management policy, framework and processes;
2. Staff performance review scores relating to risk management;
3. Insurance claims number and costs.

RISK MANAGEMENT FRAMEWORK

Council's policy is to manage risk in accordance legislative compliance requirements and with the risk management framework developed using AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines and Enterprise Risk Management – Integrated Framework (2004) Committee of Sponsoring Organisations of the Treadway Commission (COSO) as guidance material.

The relationship between the principles for managing risk, the framework in which it occurs and risk management process is shown in the following diagram.



The objective of the framework is to operationalise this policy by providing a readily accessible, usable and thorough suite of documents that enable Council and its officers to align risk management processes, people and tools. Information on framework, process and supporting tools will be provided to staff in a suite of risk management documents including a Risk Management Strategy, procedures, guidelines, templates and checklists.

The framework will be integrated with corporate planning and risk reporting processes and embedded within overall strategic and operational policies and practices.

Effective risk management will require a systematic examination of all Council activities and the places where they are carried out. The scope of risk management activities includes the following elements:

- Strategic Risk Management;

- Operational Risk Management;
- Business Continuity and Disaster Recovery Planning;
- Compliance;
- Internal Audit;
- Procurement;
- Project Risk Management; and
- Event Risk Management.

REFERENCES

Beasley, Branson and Hancock 2010 How Key Risk Indicators can Sharpen Focus on Emerging Risks Committee of Sponsoring Organizations of the Treadway Commission December 2010;

Committee of Sponsoring Organisations of the Treadway Commission 2004 Enterprise Risk Management – Integrated Framework Committee of Sponsoring Organisations of the Treadway Commission (COSO);

Corporations Act 2001 (Vic);

Department of Treasury and Finance Victoria 2011 Victorian Government Risk Management Framework Department of Treasury and Finance 2011;

Crimes Act 1958 (Vic);

Emergency Management Act 1986 (Vic)

Environment Protection Act 1970 (Vic);

Food Act 1984 (Vic);

Johnsons MME 2014 Risk Management Review Internal Audit Report Rural City of Wangaratta and Johnsons MME 2014;

Local Government Act 1989 (Vic);

Occupational Health and Safety Act 2004 (Vic);

Public Health and Wellbeing Act 2008 (Vic);

Queensland Treasury 2011 A Guide to Risk Management, The State of Queensland (Queensland Treasury) July 2011

Rittenberg and Martens 2012 Understanding and Communicating Risk Appetite;

Road Management Act 2004 (Vic)

Rural City of Wangaratta Audit Advisory Committee Charter

SAI Global 2009 AS/NZS ISO 31000:2009 Risk management - Principles and guidelines;

SAI Global 2004 HB 436:2004 Risk Management Guidelines - Companion to AS/NZS 4360:2004;

Trade Practices Act 1974 (Commonwealth);

Victorian Managed Insurance Authority 2010 Risk Management Guide Developing & Implementing a Risk Management Framework VMIA March 2010

Victorian Managed Insurance Authority 2008 Risk Management in the Victorian Public Sector Guide for developing and implementing your risk management framework Victorian Managed Insurance Authority 2008;

Wrongs Act 1958 (Vic);

REVIEW

Any change or update which materially impacts and alters this policy must be by resolution of Council on the advice of the CEO following review by the Audit Advisory Committee. Otherwise, this policy will be reviewed annually by the Audit Advisory Committee at a basic level and once every three years at a detailed level. The annual review must be included in the Committee's calendar in conjunction with a scheduled Committee meeting. Following the detailed review, recommendations will be made via CMT to Council.