Hindmarsh Shire Council

Risk Management Framework

June 2024

![Hindmarsh Shire Council logo]

Contents

1 Introduction

The purpose of this Risk Management Framework (**Framework**) is to outline how Council will implement the process for managing organisational risk into Council's overall governance, strategy and planning, management, reporting processes, policies, values and culture. The Framework also expresses Council's overall commitment to developing and maintaining and effective risk management strategies.

The framework can be used throughout the life of the organisation and can be applied to any activity, including decision-making at all levels.

Key governance influences require Council and the executive to works towards:

- **Accountability** by reporting, explaining and being answerable for the consequences of decisions it has made on behalf of the community it represents.
- **Transparenc**y by providing avenues for people to follow and understand the decision-making process.
- **Following the rule of law** by ensuring decisions are consistent with relevant legislation or common law and are within the powers of council.
- **Responsiveness** by servicing the needs of the community while.
- balancing competing interests in a timely, appropriate, and responsive manner.
- **Equity and inclusion** whereby members of the community feel their interests have been considered by Council in the decision-making process.

Effective management of risk enables Council to:

- Increase the likelihood of achieving objectives as set out in the Council Plan;
- Encourage proactive management;
- Have increased awareness of Council risks and treatment options;
- Improve the identification of opportunities and threats;
- Comply with legislative requirements;
- Improve financial reporting;
- Improve governance;
- Improve stakeholder confidence and trust;
- Establish a basis for decision making and planning;
- Improve controls;
- Improve operational effectiveness and efficiency;
- Enhance health and safety performance;
- Enhance environmental protection; and
- Improve loss prevention and incident management.

This Framework has been developed in accordance with AS/NZS ISO 31000:2018 Risk Management – Principles and Guidelines (**Guidelines**).

1.1 What is "Risk"

Risk is defined in the Guidelines as the "*The uncertainty caused by a deviation from the expected outcome. This deviation can be positive, negative or both, and can address,*

create or result in opportunities and threats" which is measured in terms of likelihood and consequence. At Council there are two broad categories of risk:

- **Strategic risks**; and

Strategic risks are risks which are generally entity wide and may impact on the ability of Council to achieve its objectives set out in the Council Plan and/or the delivery of critical services. Strategic risks should be few in number and are the critical risks for the organisation and considered in the same time horizon as the Council Plan.

- **Operational risks**.

Operational risks are risks which may impact on the achievement of directorate, business unit or service unit plan objectives.

Risk management is defined as "coordinated activities to direct and control an organisation with regard to risk".

2   Council's risk management objectives

Council's overarching objectives which have informed the development of this policy include:

- Ensuring that Council achieves the strategic objectives as set out in the Council Plan;
- Ensuring that Council is compliant with all Federal and State Government Legislation;
- Ensuring that Council's Risk Profile is prioritised according to the risks which have the capacity to do the most harm to Council;
- Establish a reliable basis for decision making and ensure that risk is included as a fundamental component in the planning process;
- Ensuring that Council has a culture which promotes proactive behaviour regarding the identification and treatment of risk; and
- Improve stakeholder confidence and trust.

3 Three Lines of Defence Model

First line of defence – The business	**Second line of defence –** Risk management and compliance	**Third line of defence –** Internal audit
• Ownership of risk and controls • Main responsibility for risk management • Risk assessments • Key risk indicators • Incident management • Issue identification and action management	• Oversight of risk management and risk profile independent from Line 1 • Compliance • Review and challenge to Line 1 • Assistance in developing risk management framework • Independent reporting escalation	• Assurance over Line 1 and Line 2 over the appropriateness, effectiveness and adequacy of the risk management framework • Independent from Line 1 and Line 2 • Recommend improvements to Line 1 and Line 2

4 Risk Governance and Responsibilities

Roles and responsibilities in the Risk Management Framework complement and expand on roles and responsibilities in the Risk Management Policy.

Role	Responsibilities
Council (Councillors)	• Council will endorse the Risk Management Policy, appropriately consider risk management issues raised in reports and make informed decisions based on the associated risks and potential opportunities. • Be satisfied that strategic risks are identified, controlled, and treated appropriately to achieve Council's strategic objectives. • Appoint and resource the Audit and Risk Committee. • Provide adequate budgetary provision for the financing of risk management including approved risk mitigation activities. • Receive reports from the Audit Committee to ensure that strategic risks are being adequately managed.
Audit and Risk Committee	The purpose of Audit and Risk Committee is to ensure Council carries out its responsibilities for accountable financial management, good corporate governance, fostering an ethical environment and maintenance of a system of internal control and risk management. They should: • Monitor, review and advise Management on the standard of its risk management. • Make assessments and recommendations in relation to Council's risk management. • Endorse and monitor a comprehensive risk based cyclical internal audit plan. The Committee is constituted to monitor and report on the systems and activities of Council in ensuring:

	- Reliable financial reporting and management information - High standards of corporate governance - Appropriate application of accounting policies - Compliance with applicable laws and regulations - Effective monitoring and control of strategic risks - Effective and efficient external and internal audit functions - Measures to provide early warning of any issues affecting the organisation's financial wellbeing - The level of effectiveness of appropriate crisis management, business continuity and disaster recovery planning. - Maintaining and fostering an ethical environment.
Internal Auditor	- The internal auditor reviews strategic risks annually as part of the development of the three-year Strategic Internal Audit Plan. - The Risk Management Framework directs the focus of audit resources to ensure higher level risks are reviewed. Risk controls and treatment plans are considered as part of each internal audit review. - Communicate independent and objective assurance and advice to management and the Audit and Risk Committee on the adequacy and effectiveness of governance and risk management (including internal control). - Satisfy legislative and regulatory expectations that serve to protect the interests of stakeholders. - The Internal Auditor liaises with the Risk Management Team to share information and knowledge.
External Auditor	External assurance providers will: - Communicate independent and objective assurance and advice to management and the Audit and Risk Committee on the adequacy and effectiveness of governance and risk management (including internal control). - Satisfy legislative and regulatory expectations that serve to protect the interests of stakeholders.
Chief Executive Officer	The CEO has the ultimate responsibility for ensuring a strong risk management culture and that risks are effectively managed across the organisation. - The Chief Executive Officer is accountable for the implementation and maintenance of risk management policies and processes across the organisation. - The Chief Executive Officer is responsible for ensuring that strategic risks are regularly reviewed. - The Chief Executive Officer is responsible for raising awareness and leading the culture of managing risk responsibly across the organisation. - Receiving and reviewing reports from management on the effectiveness of the risk management systems. - Ensuring that adequate resources are assigned to manage risk.
Executive Leadership Team	ELT will review the Risk Management Policy and amend as required.

	Operational accountability for risk culture and management as per AS ISO 31000:2018 including: • Issuing a Risk Appetite Statement. • Reviewing Council's Risk Management Policy. • Ensuring necessary resources are allocated to risk management. • Assigning authority, responsibility, and accountability at appropriate levels. • Actively promoting and supporting the desired risk culture. • Determining risk-taking limits and targets for their departments within the policies and guidelines established by Council and SMT through this framework. • Ensuring any strategic risks allocated to their division are actioned, monitored and reported on. • Establishing risk management processes tailored for their sphere of responsibility. • Ownership of the risk-taking and risk management decisions taken in the performance of their activities. • Apply this framework in the identification, assessment, management, monitoring and reporting of risks, including appropriate assessment of the impact of new products, projects and processes.
Senior Management Team	Senior Managers will: • Understand, cascade, and operationalise risk management throughout the organisation. • Execute effective internal control in their functional areas, as well as the monitoring of process and maintaining transparency in the internal control itself. • Accountable for implementing the risk management framework in their area of responsibility. This includes ensuring that risks are identified, evaluated, reviewed, and updated regularly. • Perform and coordinate periodic control self-assessments to validate control effectiveness ratings. • Ensure that assets and operations, together with liability risk to the community, are adequately protected through treatment plans and measures. • Provide risk management related information as requested by their Directorate. • Managers are responsible for raising awareness and leading the culture of managing risk responsibly across the organisation by ensuring that risk management policies, procedures, standards, guidelines, and risk management treatment plans are implemented in everyday business practice. • SMT is responsible for monitoring operational risks. • Monitoring quarterly reports from Risk Management which include operational and strategic risk register actions, insurance claims and trends.
Team Leaders and Coordinators	• Advising of any risk management matter that should be included in budgets and business planning.

	• Are responsible for raising awareness and leading the culture of managing risk responsibly across the organisation by assisting with the implementation of risk management policies, procedures, standards, guidelines, and risk treatment plans.
People and Performance Team	The risk management and compliance functions will: • Responsible for overseeing the development of facilitation and implementation of the Risk Management Framework through responsibility for risk management development, monitoring processes and the implementation of the organisations overall risk management. • Supporting Council staff with their risk management obligations and providing staff with advice and tools to ensure risk management compliance. • Monitor and report to ELT on the organisation's exposure to risk. • Provide advice to the organisation and are responsible for Strategic Risk overview and periodic reporting to the Audit and Risk Committee.
All Employees	• Employees are responsible for taking all reasonable care to prevent loss, maximise opportunity and to ensure that Hindmarsh Shire Council operations, reputation and assets are not adversely affected. • Employees must be aware of and understand the risks associated with their actions and comply with the risk management policy, supporting guidance and procedures. • Immediately report risk exposure and losses to supervisors and where possible act to mitigate any further loss. • Identify new risks to their area of accountability and report those risks appropriately.

5   Risk Appetite

Risk appetite is the amount of risk exposure, or potential adverse impact from an event, that Hindmarsh Shire Council is willing to accept in the pursuit of its objectives. Council maintains a Risk Appetite and Tolerance Statement that details the types and amounts of risk that Council is willing to accept in pursuit of its strategic objectives.

Once the risk appetite threshold has been breached, risk management controls and actions are required to bring the exposure level back within the accepted range.

Council's overarching Risk Appetite Statement is as follows:

Hindmarsh Shire Council's risk appetite is 'Cautious'. Council will consider options and choose one that is safe, but also may maximise its ability to innovate, deliver strategic priorities and services, and care for the safety and wellbeing of staff, while also providing an acceptable level of reward and value for the community it serves and for local government.

Risks will be managed in line with Hindmarsh Shire Council's risk appetite and risk tolerance scales and will be considered in all decision making and planning.

The Risk Appetite Statement summarises the Council's tolerance for risk in each of a whole range of activities it undertakes. For example, the Council's tolerance for risk in health and

safety matters is very low; hence a highly cautious (low) appetite for that category. On the other hand, tolerance for risk in service delivery is conservative (relatively moderate). All of the activities undertaken by Council can be so classified in terms of risk appetite.

Hindmarsh Shire Council has a level of risk appetite that it tolerates which is low, medium and high as detailed in the table below:

Risk rating	Minimum treatment required	Description
Extreme (review monthly)	Reject or mitigate	Extreme risk is unacceptable. Immediately consider whether the activity associated with this risk should cease. Comprehensive consideration by ELT required to ensure the risk is consistent with corporate objectives and risk appetite. Any decision to continue exposure to this level of risk should be made at ELT/ Audit and Risk Committee / Council level, be subject to the development of detailed treatments, on-going oversight, and high-level review. Detailed research and planning required to mitigate risk.
High risk (review quarterly)	Accept and mitigate	Risk should be reduced by developing treatments. It should be subject to on-going review to ensure controls remain effective, and the benefits balance against the risk. Escalation of this level of risk to Director level should occur. Attention required to assess the acceptability of remaining risk or required mitigation measures. Management to ensure that necessary risk mitigation improvement strategies are implemented, and the risk does not increase by actively monitoring the control environment.
Medium risks (review half yearly)	Accept	Exposure to the risk may continue, provided it has been appropriately assessed and has been managed to as low as reasonably practicable. It should be subject to frequent review to ensure the risk analysis remains valid and the controls effective. Treatments to reduce the risk can be considered. Risk Owner to ensure that the control environment does not substantially change. Consider the implementation of any additional cost-effective controls.
Low risks (review annually)	Accept	Exposure to this risk is acceptable but is subject to periodic review to ensure it does not increase and current control effectiveness does not vary. Manage by routine procedures and be mindful of changes to nature of risks. Consider the implementation of any cost-effective internal controls.

Detailed information around the acceptance of particular risk categories is contained within the detailed Risk Appetite and Tolerance Statement.

6   AS/NZS ISO 3100: 2018 Risk Management – Principles and Guidelines

Hindmarsh Shire Council has adopted the following risk management principles, framework and processes from AS/NZS ISO 3100: 2018 Risk Management – Principles and Guidelines.

6.1   Risk Management Principles

Council is guided by the following risk management principles outlined in AS/NZS ISO 3100: 2018 Risk Management – Principles and Guidelines:

- Risk management creates and protects value.
- Risk management is an integral part of all organisational processes.
- Risk management is part of decision making.
- Risk management explicitly addresses uncertainty.
- Risk management is systemic, structured and timely.
- Risk management is based on the best available information.
- Risk management is tailored.
- Risk management takes human and cultural factors into account.
- Risk management is transparent and inclusive.
- Risk management is dynamic, iterative and responsive to change.
- Risk management facilitates continual improvement of the organisation.

7   Risk Management Framework

The key elements of the risk management framework are as follows:

Mandate and commitment – Council has a strong and sustained commitment by management to ensure the ongoing effectiveness of risk management in Council. This commitment should support the development of a positive risk culture within the agency.

Implementing risk management – the risk management process is applied through a risk management plan at all relevant levels and functions of the department or agency as part of its practices and processes. Investment in resources and capabilities will enable Council to effectively and efficiently apply its risk management activities.

Monitoring and review of the framework – Council should continually ensure that risk management is effective and supports organisational performance. The risk management framework is to be reviewed annually and enhanced as required.

7.1   Risk management process
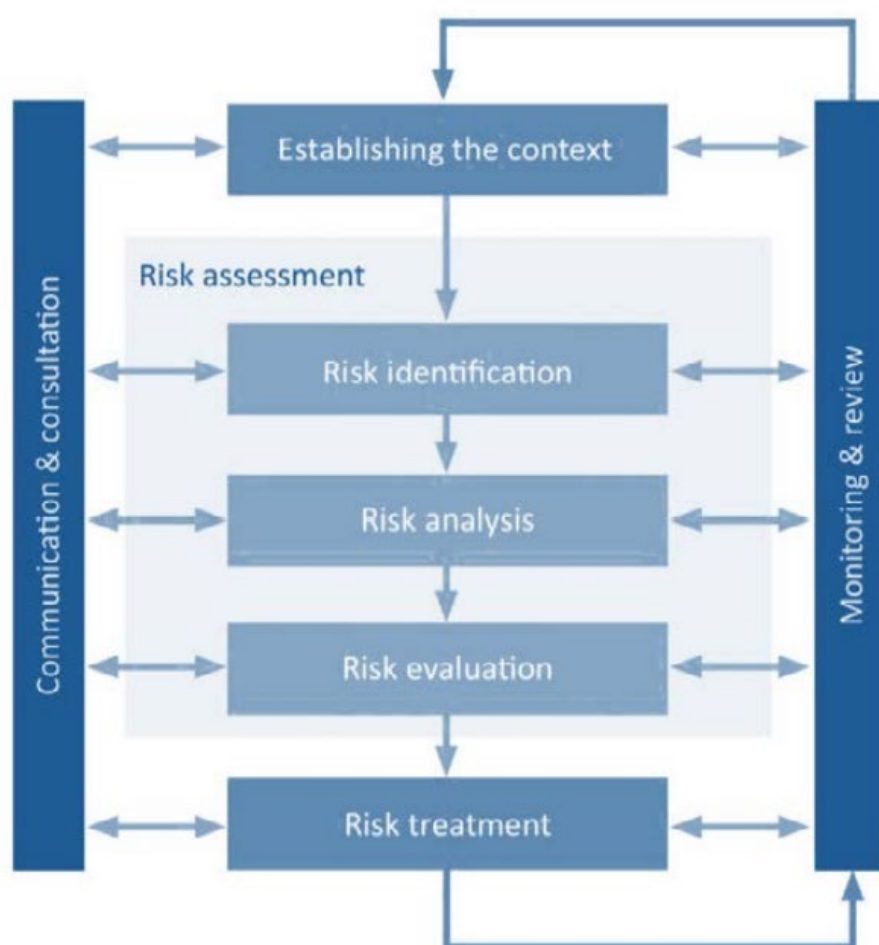
The key elements of a risk management process are as follows:

- ***Establish the context*** means understanding Council's objectives, defining internal and external factors that could be a source of uncertainty, helping identify risk and setting the scope and risk criteria for the remaining risk management process.
- ***Risk identification*** determines what, where, when, why and how risks could arise, and the effect this would have on an agency's ability to achieve its objectives. A range of government and industry resources may be employed to assist in the identification of risks. Risks may also be investigated through community engagement sessions.

- *Risk analysis* determines the risk level against the risk criteria by understanding how quickly a risk can occur, the sources and cause of a risk, the consequences and likelihood of those consequences. Analysis takes into account the effectiveness of existing controls. Risk evaluation compares the level of risk against the risk criteria and considers the need for treatment. The approach to risk evaluation should follow a typical risk assessment process of applying a consequence and likelihood matrix. Assessing the risks in relation to each other supports prioritisation and highlights differences. Mitigation strategies can be taken into account to derive the residual risk.
- *Risk treatment* involves assessing and selecting one or more options for modifying risks by changing the consequences or likelihood and implementing selected options through a treatment plan.
- *Communication and consultation* takes place throughout the risk management process with all identified stakeholders to ensure those accountable for implementing the risk management process and stakeholders understand the basis on which decisions are made.
- *Monitoring and review* confirms that risk and the effectiveness of control and risk treatments are monitored and reported to ensure that changing context and priorities are managed and emerging risks identified.

8 Reporting

There is a structured approach to risk reporting. The matrix below details which information will be reported throughout the organisation together with the reporting frequency. All Strategic and Operational risks are available for review via Riskware. Timelines for review are dependent on the Strategic or Operational residual risk rating populated in Riskware. Management receive an alert in Riskware when a Strategic or Operational risk requires review based on the residual risk rating, the controls, or treatment plan required.

Risk Report or Update	Audit and Risk Committee	ELT	SMT
Strategic	As per Work Plan	March, June, Sept.	Monthly
Operational	As per Work Plan	March, June, Sept.	Annually
Risk Trends	As per Work Plan	Quarterly	Quarterly

9 Risk Management Maturity

Risk maturity describes risk capability and the level of sophistication an organisation operates at in terms of its risk processes and procedures. Risk maturity is not a static concept and should be tailored to reflect how risk can best support delivery of strategic objectives.

The extent to which an organisation implements the following key elements of an enterprise-wide Risk Management system will assist in the determination of its maturation status:
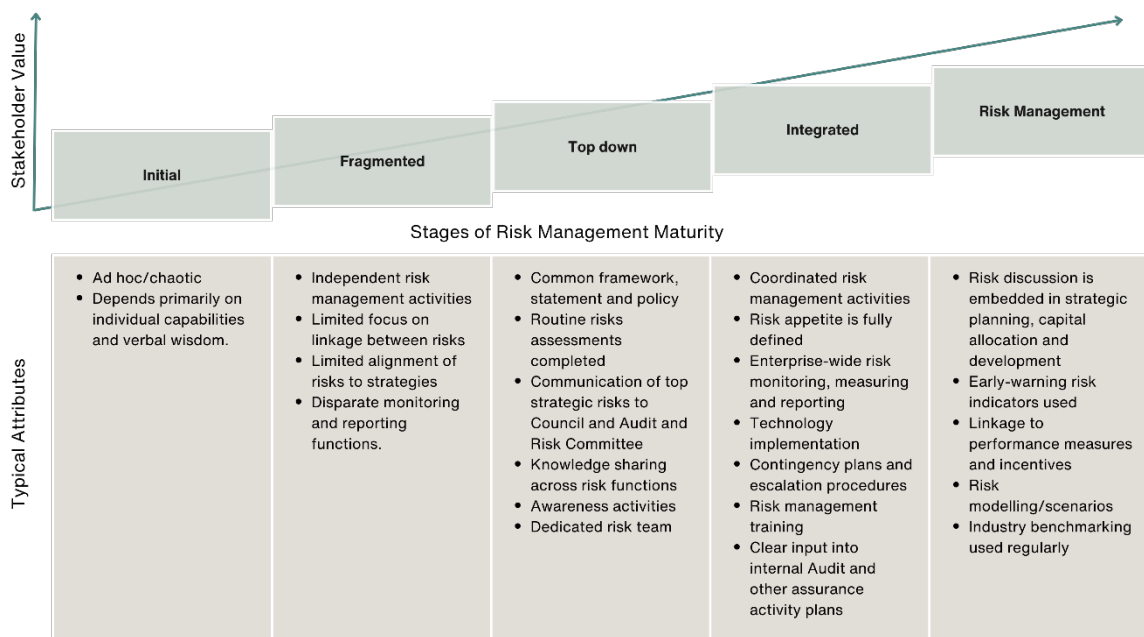
- The risk management process has been applied appropriately and all elements of the process are suitable and sufficient.
- The risk management process is in keeping with the strategic needs and intent of the organisation.
- All significant risks have been identified and are being treated.

- Controls are being correctly designed in keeping with the objectives of the risk management process.
- Critical controls are adequate and effective.
- Review by line management and other non-audit assurance activities are effective at maintaining and improving controls.
- Risk treatment plans are being executed.
- There is appropriate and as-reported progress in the risk management plan.

Council has committed to a path of continuous improvement to deliver and embed an optimum Risk Management Framework within our organisation to equip the business with the right skills and capabilities to manage risk to achieve our strategic aims as documented in the Council Plan. Council continues to improve in its realisation of a mature and integrated enterprise-wide Risk Management Framework.

The stages of Enterprise-wide Risk Management Maturity are depicted on the following page.

Stages of Risk Management Maturity

Initial	Fragmented	Top down	Integrated	Risk Management
• Ad hoc/chaotic • Depends primarily on individual capabilities and verbal wisdom.	• Independent risk management activities • Limited focus on linkage between risks • Limited alignment of risks to strategies • Disparate monitoring and reporting functions.	• Common framework, statement and policy • Routine risks assessments completed • Communication of top strategic risks to Council and Audit and Risk Committee • Knowledge sharing across risk functions • Awareness activities • Dedicated risk team	• Coordinated risk management activities • Risk appetite is fully defined • Enterprise-wide risk monitoring, measuring and reporting • Technology implementation • Contingency plans and escalation procedures • Risk management training • Clear input into internal Audit and other assurance activity plans	• Risk discussion is embedded in strategic planning, capital allocation and development • Early-warning risk indicators used • Linkage to performance measures and incentives • Risk modelling/scenarios • Industry benchmarking used regularly

10   Training and Education
Risk management training and awareness is recognised as an important requirement for all staff. Training shall be designed to increase the knowledge and awareness of staff and management in several risk management topics including general risk management, liability, fraud awareness, environment, events, and Business Continuity. In addition to formal training the Risk Management Team act as specialist advisors to staff. This includes help with identifying and assessing risk exposures and the steps in developing, implementing, and monitoring of sustainable control measures.

11   Related Documents

Internal documents	External documents (legislation, Australian Standards)

Hindmarsh Shire Council Risk Management Policy Hindmarsh Shire Council Risk Appetite and Tolerance Statement Hindmarsh Shire Council Plan (as adopted) Hindmarsh Shire Council Fraud Prevention and Control Policy and Plan	AS/NZS ISO 31000:2018 Risk Management Principles and Guidelines

12   Document Control

Risk Management Framework			**Policy Category**	Council
Version Number	1.3		**Policy Status**	Draft
Approved/Adopted By	COUNCIL		**Approved/Adopted on:**	
Responsible Officer	DCCS		**Review date:**	
Version History	**Date**	**Version**	**Description**	
	June 2013	1.0	Initial Risk Management Strategy	
	May 2021	1.1	Risk Management Framework	
	June 2024	1.2	Risk Management Framework presented to Audit and Risk Committee	
	July 2024	1.3	Risk Management Framework presented to Council.	