LODDON SHIRE COUNCIL

RISK MANAGEMENT FRAMEWORK

LODDON
SHIRE

DOCUMENT INFORMATION

DOCUMENT TYPE:	Strategic document
DOCUMENT STATUS:	Approved
POLICY OWNER POSITION:	Director Corporate
INTERNAL COMMITTEE ENDORSEMENT:	Audit and Risk Committee
APPROVED BY:	Council
DATE ADOPTED:	23 /01/2024
VERSION NUMBER:	4
REVIEW DATE:	23/01/2028
DATE RESCINDED:	
RELATED STRATEGIC DOCUMENTS, POLICIES OR PROCEDURES:	Risk Management Policy Risk Appetite Statement Risk Management Procedure Risk Management Implementation Plan Occupational Health and Safety Policy Fraud and Corruption Prevention Policy Fraud and Corruption Control Plan ISO31000:2018 Risk Management - Guidelines Occupational Health and Safety Plan
RELATED LEGISLATION:	Local Government Act 2020 Occupational Health and Safety Act 2004 Occupational Health and Safety Regulations 2017
EVIDENCE OF APPROVAL:	Signed by Chief Executive Officer
FILE LOCATION:	K:\EXECUTIVE\Strategies policies and procedures\Strategies - adopted PDF and Word\STR Risk Management Framework v4.docx

Strategic documents are amended from time to time, therefore you should not rely on a printed copy being the current version. Please consult the Loddon Shire website to ensure that the version you are using is up to date.

This document is available in alternative formats (e.g. larger font) if requested.

CONTENTS

1 PURPOSE

The purpose of this framework is to document:

- the principles of Loddon Shire Council's risk management system, commitment to risk management and how that operates internally
- the roles and responsibilities of risk management within Council
- the reporting structures that provide the Council with the appropriate oversight of risk management within the organisation.

Council's Risk Management Policy includes a commitment to: "Assign authority, responsibility and accountability for managing risk at appropriate levels within the organisation and document this in the Risk Management Framework which outlines how risk management aligns to ISO31000:2018."

2 INTRODUCTION

Loddon Shire Council has developed a risk management system that includes:

- Risk Management Policy
- Risk Management Framework (this document)
- Risk Management Implementation Plan
- Risk Appetite Statement
- Risk Management Procedure.[1]

The framework has been developed in line with *ISO 31000:2018*, the Australian Standard for risk management. Council's approach to risk management and how that links to the Standard have been addressed in the framework.

The definition of risk in *ISO 31000:2018* is "effect of uncertainty on objectives."[2] The Standard further notes "An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats."[3]

As Council's risk maturity increases, the opportunity side of risk will be incorporated into the Risk Management Policy and this framework. For now, this framework is focussed on progressing risk management maturity on the threat side of risk.

3 SCOPE

The Risk Management Framework incorporates all risks faced by Council in achieving its strategic objectives during normal operations. They are categorised as strategic, operational and project risks.

Monitoring and reporting activities that are captured under the Road Management Act 2004 have been excluded from this framework, as they have their own monitoring and reporting requirements embedded in Council's Road Management Plan.

4 RISK MANAGEMENT OBJECTIVES

Effective risk management promotes an environment where everyone can make informed decisions that support achievement of Council's vision and strategic objectives.

[1] Risk Management Procedure development in progress

[2] Standards Australia Limited, *ISO Australian Standard 31000:2018 Risk Management – Guidelines, p1*

[3] Standards Australia Limited, *ISO Australian Standard 31000:2018 Risk Management – Guidelines, p1*

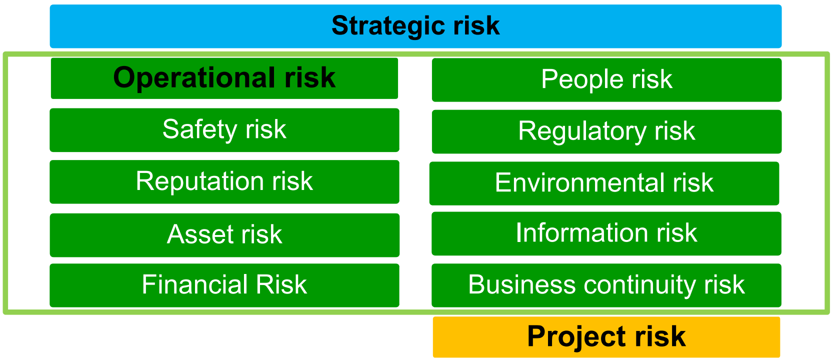
The objectives for risk management include:

- identifying and preparing for uncertain events to reduce their impact should they arise
- supporting achievement of strategic objectives
- ensuring responsibilities and accountabilities are clearly defined
- making the necessary resources and training is available to promote a risk aware organisation
- embedding risk management into everything we do so that it becomes second nature
- promoting a risk culture across the organisation.

If we can achieve these objectives, good risk management will lead to increased performance.

5 TYPES OF RISK

Council is a complex business with a variety of services, programs, and projects. The following risk categories and types are those prevalent to Council.



This framework identifies Strategic Risk, Operational Risk, and Project Risk as the three key categories of risks. The risk management approach for each risk group is identified in this framework.

5.1 Strategic risks

Strategic risks:

- are those risks that can cause a shift in Council's strategic objectives
- can have a long-term impact or be ongoing
- are those impacted in the most part by external events.

5.2 Operational Risks

Operational risks:

- relate to the delivery of services and programs
- can have short-term or long-term impact, or be ongoing
- are those impacted by internal or external events.

5.3 Project risks

Project risks:

- relate to the delivery of specific projects, and are the risk of an uncertain event or condition having an effect on project outcomes
- impact the project itself, and the life of the risk is limited to project delivery
- are those impacted by internal or external events.

6 ISO31000:2018 RISK MANAGEMENT – GUIDELINES

Council's Risk Management Policy and Risk Management Framework are the foundation documents that outline Council's commitment to risk management. The policy and framework are aligned to the *ISO 31000:2018*, which articulates the principles, framework, and processes for achieving best practice in risk management, as per Figure 1[4].

The Standards are considered best practice documents, and used widely to provide a consistent guide on a particular topic.[5]

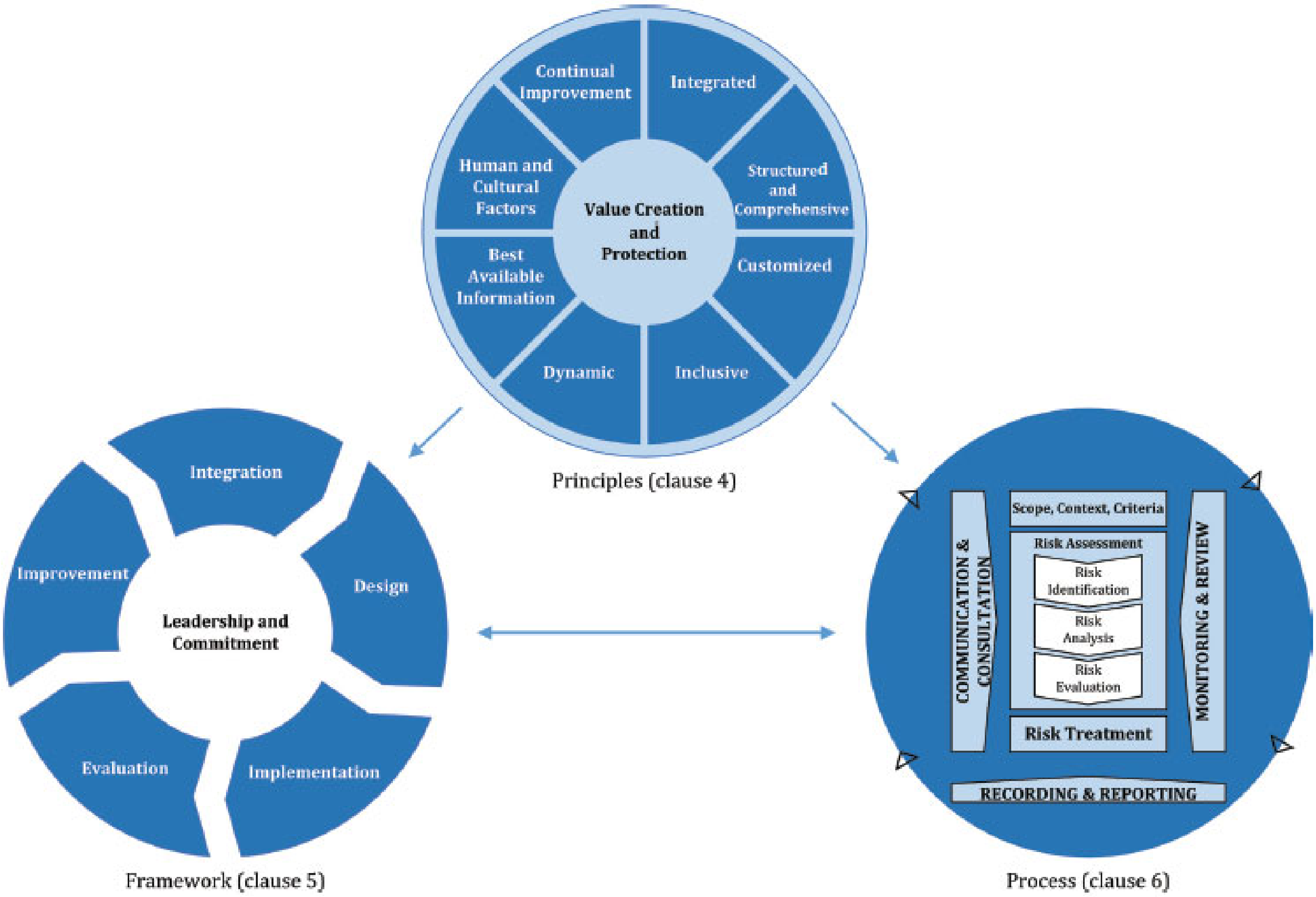


Figure 1 — Principles, framework and process

[4] Standards Australia Limited, *ISO Australian Standard 31000:2018 Risk Management – Guidelines, pv*

[5] ISO (International Organisation for Standardization) is an independent, non-governmental international organisation with membership from national standard bodies. It brings together experts to share knowledge and develop International Standards that support innovation and provide solutions to global challenges (https://www.iso.org/about-us.html, Accessed: 9 March 2022)

7 PRINCIPLES

The principles outlined in Figure 2 provide guidance on the characteristics of effective and efficient risk management, communicating its value and explaining its intention and purpose. The principles are the foundation for managing risk[6].

Each of the principles must be evidenced for Council to be implementing effective and enterprise-wide risk management and will serve as points of reference for periodically reviewing the maturity of risk management at Council. The principles are:

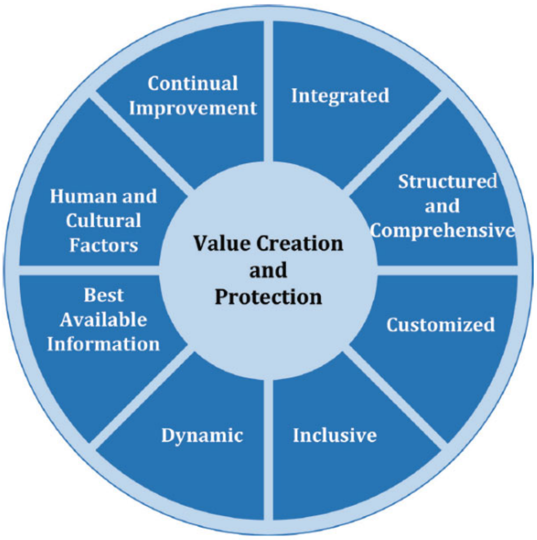

Continual Improvement
Integrated
Structured and Comprehensive
Customized
Inclusive
Dynamic
Best Available Information
Human and Cultural Factors
Value Creation and Protection

Figure 2 — Principles

a) **Integrated**: Risk management is an integral part of all activities.
b) **Structured and comprehensive**: A structured and comprehensive approach to risk management contributes to consistent and comparable results.
c) **Customised:** The risk management framework and process are customised and proportionate to the external and internal context related to Council's objectives.
d) **Inclusive**: Appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management.
e) **Dynamic:** Risks can emerge, change or disappear as the external and internal context changes. Risk management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner.
f) **Best available information**: The inputs to risk management are based on historical and current information, as well as on future expectations. Risk management explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information is timely, clear and available to relevant stakeholders.
g) **Human and cultural factors**: Human behaviour and culture significantly influence all aspects of risk management at each level and stage.
h) **Continual improvement**: Risk management is continually improved through learning and experience[7].

When these attributes are evidenced in the organisation, Council will have a high level of risk maturity. The Risk Management Implementation Plan will assist in developing and monitoring this maturity over time.

[6] Standards Australia Limited, *ISO Australian Standard 31000:2018 Risk Management – Guidelines,* p3

[7] Standards Australia Limited, *ISO Australian Standard 31000:2018 Risk Management – Guidelines,* p3

8 FRAMEWORK

The purpose of the risk management framework is to assist Council in integrating risk management into significant activities and functions.

The effectiveness of risk management will depend on its Implementation into the governance of Council, including decision-making.[8] The framework elements are:

8.1 Leadership and commitment

8.1.1 Governing body

Council is ultimately responsible for risk management, and discharges the day-to-day responsibility for risk to management.

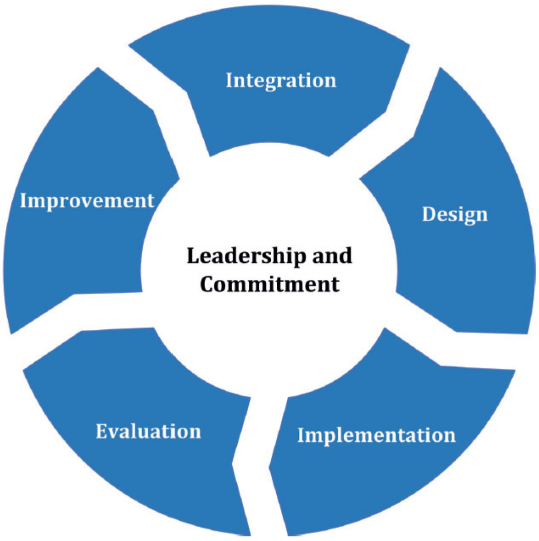


Figure 3 — Framework

Under the Local Government Act 2020 (The Act), Section 53 mandates establishment of an Audit and Risk Committee by Council. This Council has an active Audit and Risk Committee, which has oversight responsibility for risk management on behalf of the Council.

Council evidences its commitment to risk management through the reporting structure that ensures a summary of all Audit and Risk Committee Meetings are reported to the Council. It also ensures that risk related documents, such as the Risk Management Policy, this framework, Risk Appetite Statement and Risk Management Implementation Plan, are endorsed by the Audit and Risk Committee before approval by Council.

8.1.2 Operations

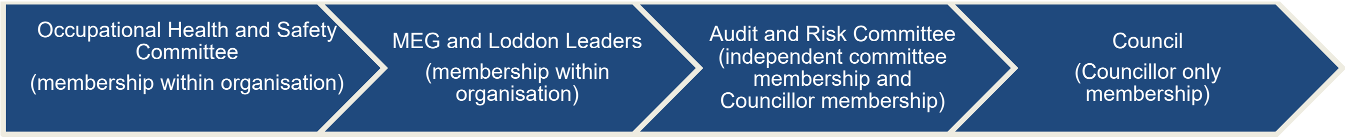
Risk management is fully supported and endorsed by Council's Management Executive Team (MEG) and Loddon Leaders (management). These groups play an integral leadership role in the organisation.

8.2 Integration

It is stated in *ISO 31000:2018* that ***everyone in an organisation has responsibility for managing risk***.

Council's approach provides an integrated model for risk management with responsibilities, with Council as the highest authority, through the layers of the organisation to individual teams who operate in a risk-focused environment.

The meeting structure for the various reporting lines for risk management has been coordinated to ensure that information flows from the ground roots of the organisation all the way to the Council. Its implementation is as follows:


Occupational Health and Safety Committee
(membership within organisation)
MEG and Loddon Leaders
(membership within organisation)
Audit and Risk Committee
(independent committee membership and Councillor membership)
Council
(Councillor only membership)

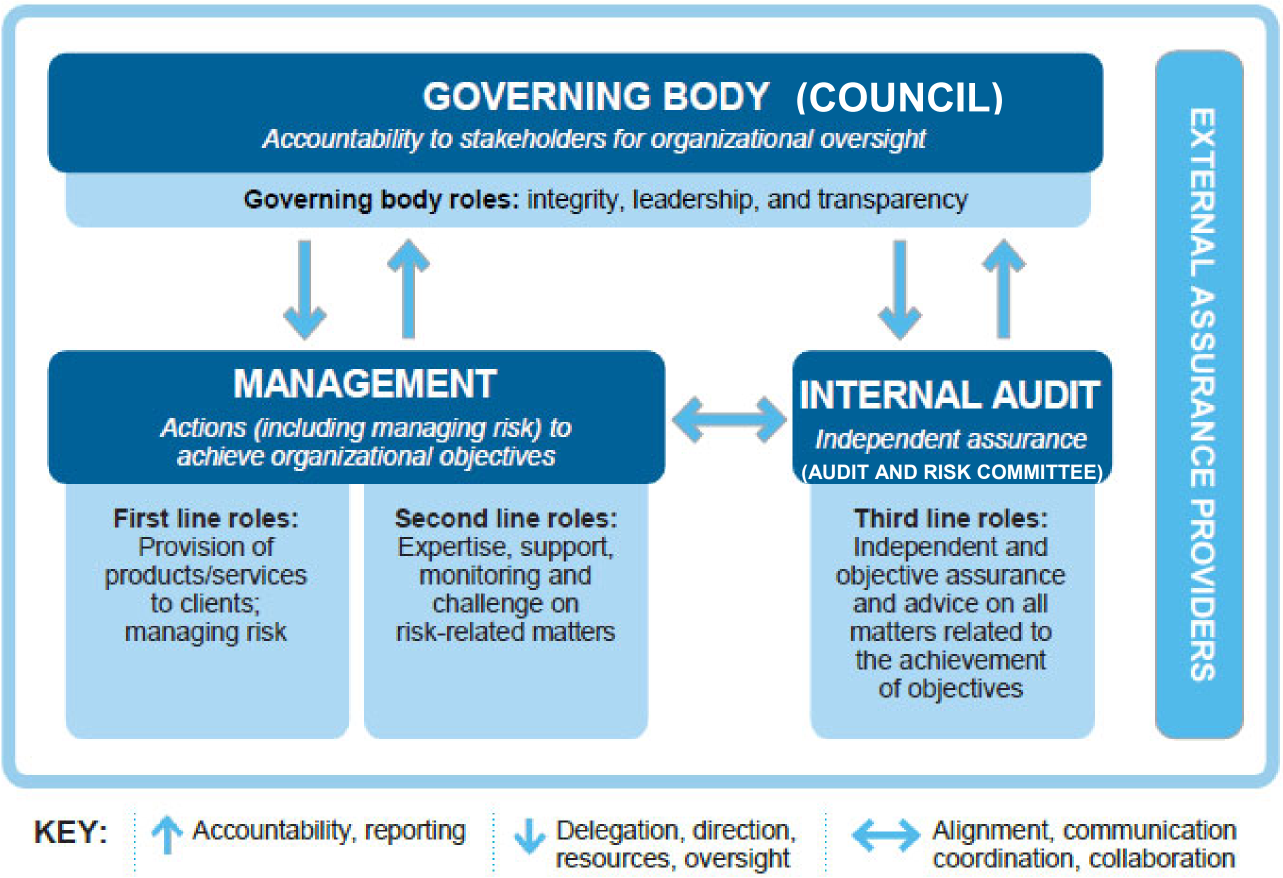
[8] Standards Australia Limited, *ISO Australian Standard 31000:2018 Risk Management – Guidelines,* p4

Integration is further achieved through Council's internal control environment, which is based on the three lines model in managing risk.

The three lines model incorporates:

1. Management controls and internal control measures (own and manage the risks).
2. Financial controls, risk management processes, quality controls, security (such as delegations), inspection and compliance (oversee risks).
3. Assurance oversight (internal and external audit).

This diagram[9] models Council's governance framework through the three lines model, which ensures Council is included in the reporting and awareness structure through the Audit and Risk Committee.


GOVERNING BODY (COUNCIL)
Accountability to stakeholders for organizational oversight
Governing body roles: integrity, leadership, and transparency
MANAGEMENT
Actions (including managing risk) to achieve organizational objectives
First line roles: Provision of products/services to clients; managing risk
Second line roles: Expertise, support, monitoring and challenge on risk-related matters
INTERNAL AUDIT
Independent assurance
(AUDIT AND RISK COMMITTEE)
Third line roles: Independent and objective assurance and advice on all matters related to the achievement of objectives
EXTERNAL ASSURANCE PROVIDERS
KEY:
Accountability, reporting
Delegation, direction, resources, oversight
Alignment, communication coordination, collaboration

[9] https://www.iia.org.au/technical-resources/professionalGuidance/the-iia's-three-lines-model Accessed: 11 May 2022.

8.2.1 The first line: operational management

As the first line, managers own and manage risks and are responsible for implementing mitigating actions to address process and control deficiencies.

They are accountable for the maintenance of effective internal controls and for executing risk and control procedures on a day-to-day basis.

Management identifies, assesses, controls, and mitigates risks, guiding the development and implementation of internal policies and procedures and ensuring that activities are consistent with goals and objectives.

This information is reported through Loddon Leaders quarterly compliance meetings.

8.2.2 The second line: oversee risks

The second line comprises various risk management and compliance functions to help build, maintain and monitor the first line controls.

Functions include:

- risk management functions by management that assist risk owners in identifying and analysing risks in their areas of the organisation, ensuring they are monitored and acted upon when they are outside tolerance, and reported in accordance with documented procedures
- compliance functions to monitor various specific risks such as noncompliance with applicable laws and regulations, finance, governance, procurement, occupational health and safety and project management.

Specific responsibilities of these functions include:

- identifying and recording emerging risks
- monitoring existing risks
- following the risk management framework protocols
- adhering to policies and procedures
- identifying shifts in Council's internal and external environment
- responding to emerging issues and changing regulatory risks
- undertaking training on risk management processes
- assisting in the development of processes and controls to manage risks.

This information is reported through Loddon Leaders and the Audit and Risk Committee.

8.2.3 The third line: internal audit

The internal audit function provides Council and management with comprehensive assurance based on the highest level of independence and objectivity.

This function is overseen by the Audit and Risk Committee and provides assurance on the effectiveness of governance, risk management, compliance, and internal controls, including the manner in which the first and second lines achieve risk management and control objectives.

The function actively contributes to effective organisational governance providing best practice conditions are met, such as:

- the function is independent (external contractor)
- it performs its role in accordance with recognised international standards for the practice of internal auditing
- it reports and is able to perform its duties independently, reporting through to the Audit and Risk Committee, which has independent membership
- it has an active link to Council via Councillor membership on the Audit and Risk Committee and biannual reporting to Council.

In addition to the internal audit function, the Audit and Risk Committee reviews the annual Financial Statements and Performance Statement, which are audited by the Auditor-General Victoria's contractor; sometimes referred to as the fourth line.

This information is reported to the Audit and Risk Committee and the Council.

8.3 Design

8.3.1 Understanding the organisation and its context

Council is a complex business, and has significant external contexts under which it operates. This was prevalent with the global spread and impact of COVID-19 across the world, and at a very local level.

ISO31000:2018 includes "social, cultural, political, legal, regulatory, financial, technological, economic and environmental factors, whether international, national, regional or local"[10] and each of these are relevant to Council's business.

Internally, Council operates in a highly regulated environment, and that is reflected in many of the internal contexts identified below. In many ways, a regulated environment can be easier to implement frameworks such as this Risk Management Framework because roles, responsibilities, accountabilities and delegated authorities are very clear, and easy to communicate.

"Internal context may include, but is not limited to:

- Council's vision, mission and values;
- governance, organisational structure, roles and accountabilities;
- strategy, objectives and policies; culture;
- standards and guidelines adopted by the organisation;
- capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, intellectual property, processes, systems and technologies);
- data, information systems and information flows;
- relationships with internal stakeholders, taking into account their perceptions and values; contractual relationships; and
- commitments."[11]

The consequence table in the Risk Management Policy has various consequence types associated with Council's operations which address many of the contextual items listed.

8.3.2 Articulating risk management commitment

Council's commitment to risk management is articulated in the governance structure whereby Council is the approval authority for all key risk documents such as the Risk Management Policy, this framework, Risk Management Implementation Plan, and Risk Appetite Statement. Review and approval of these documents provides Council with the appropriate oversight of risk within the organisation.

8.3.3 Assigning organisational roles, authorities, responsibilities and accountabilities

The roles and responsibilities for risk management are provided in the Local Government Act 2020, Council's committee charters and terms of reference, and positions descriptions for staff. They are fully documented in Section 9: Roles and Responsibilities within this framework.

[10] Standards Australia Limited, *ISO Australian Standard 31000:2018 Risk Management – Guidelines,* p6

[11] Standards Australia Limited, *ISO Australian Standard 31000:2018 Risk Management – Guidelines,* p6

8.3.4 Allocating resources

The Director Corporate is the key resource for risk management, supported by the Governance Team. This team oversees risks under the “governance-risk-compliance” spectrum, which includes broad corporate risks and regulatory risk.

Council’s Manager Governance is responsible for facilitating a culture of best practice in safety risk management (OH&S) across the organisation.

However, risk management is everybody’s responsibility at Council and this requires an ongoing awareness of the environment. The Director Corporate, supported by the Governance Team, assists teams with identification and assessment of their risks and development of risk registers. Managers are available to support their teams to increase their awareness and knowledge of risk management relevant to their area of operations.

8.3.5 Establishing communication and consultation

The importance of communication and consultation around risk management cannot be underestimated. It serves as a preventative tool, and a response tool as a learning activity where incidents are reported back to the organisation.

To ensure risk management is communicated broadly across the organisation:

- there are online learning and development modules targeted at specific risk areas (such as fraud and corruption, privacy, etc.)
- risk management documents are available from the intranet and communicated to staff periodically, including during and following their review
- Governance team submits items for the staff newsletter to increase awareness
- there are safety conversations at team levels
- there is an Occupational Health and Safety Plan, an Occupational Health and Safety webpage, and an annual learning and development calendar that captures safety compliance training
- there is a Health and Wellbeing webpage on the intranet, and an annual calendar promoting health and wellbeing initiatives.

8.4 Implementation

Everyone within Council has a role within the risk management program, and is encouraged to identify risks and have them registered and reported through the appropriate channels.

Specifically, the Council, through the Local Government Performance Reporting Framework, is responsible for identifying its strategic risks to Council’s operations, their likelihood and consequences of occurring and risk minimisation strategies for those risks.

The Audit and Risk Committee has oversight of the governance, compliance and risk environment, and ensuring that the internal control environment is sufficient, and where it needs improving, recommending inclusion of internal audit reviews in the Strategic Internal Audit Plan.

Loddon Leaders has the responsibility to promote a culture of risk management throughout the Council by:

- actively identifying and assessing current and emerging risks and ensuring they are accurately reflected in the Operational Risk Register
- embedding a risk management culture across the organisation through their actions and advocacy for the risk management program
- providing advice on continual improvement of the management of risk.

The Director Corporate has the ultimate organisational responsibility for the risk management program ensuring:

- all risk management documents are reviewed and updated through the authorising environment
- any risks outside appetite are escalated, as per Section 9.5: Monitoring and Review of this framework
- reporting is provided to Loddon Leaders, the Audit and Risk Committee, and Council.

The Manager Governance is responsible for occupational health and safety risk and promoting a safety culture.

Project managers and project officers are responsible for managing risks related to their specific projects.

8.5 Evaluation

The core risk management documents are subject to regular review to ensure they remain relevant for Council's operations. The Risk Management Implementation Plan, which is the plan to drive continuous improvement in risk management, is subject to annual review to ensure completion of current actions and develop new actions to increase risk maturity at Council. During its review, the effectiveness of the risk management program is evaluated to ensure activities are adding value, and risk management maturity is increasing.

8.6 Improvement

8.6.1 Adapting

Council reviews strategic risks every six months to understand any changes to the internal or external context.

The Audit and Risk Committee annually reviews the Strategic Internal Audit Plan, a risk based plan that identifies internal audit reviews that address the most significant risks and/or add the best value to Council's operations.

Loddon Leaders assesses emerging operational risks from changes to the external and internal environment, and ensures that risk assessments are undertaken for newly identified risks.

Project managers and project officers have an ongoing role throughout the life of projects to ensure that the internal and external context is reviewed and risks assessed accordingly.

8.6.2 Continually improving

The Risk Management Implementation Plan identifies actions to increase Council's risk management maturity under the headings of:

- Risk management framework
- Risk management process
- Risk culture.

The actions in the plan will progressively be completed, and progress will be reported back to Council via the Audit and Risk Committee.

The plan will be reviewed periodically to ensure new actions are captured and monitored. In the same way, the core risk management documents are subject to regular review to ensure they remain relevant for the Council.

9 PROCESS

"The risk management process should be an integral part of management and decision-making and integrated into the structure, operations and processes of the organisation. It can be applied at strategic, operational, programme or project levels."[12] The elements of the process are:

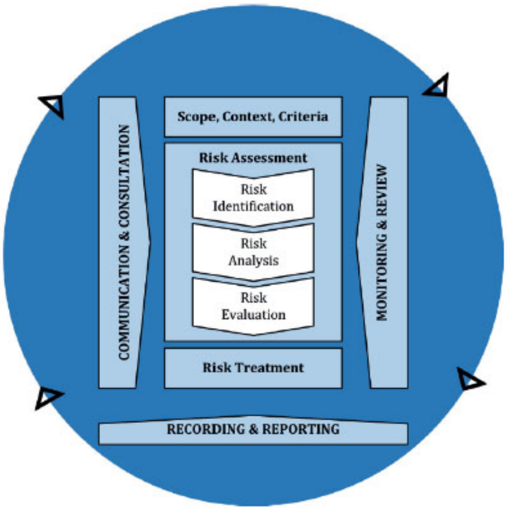


Figure 4 — Process

9.1 Communication and consultation

Communication of the risk management process is a fundamental part of best practice risk management and of an enterprise risk management framework.

Section 8.3.5 identifies the communication and consultation mechanisms.

9.2 Scope, context and criteria

9.2.1 Defining the scope

The Council, through the Local Government Performance Reporting Framework, is responsible for identifying its strategic risks to Council's operations, their likelihood and consequences of occurring and risk minimisation strategies for those risks.

In accordance with the Act, the Council has provided the Audit and Risk Committee with responsibility for overseeing risk management. Specifically, the Committee is responsible for overseeing strategic risks and operating risks.

Loddon Leaders is responsible for assessing operating risks.

Council officers are also responsible for identifying and assessing operational and project risks in their area of Council operations.

Project managers and project officers are responsible for assessing project risks.

The Manager Governance is responsible for ensuring relevant corporate frameworks exist to support Council's compliance with Occupational Health and Safety related legislation and regulations and provide advice and support to staff on health and safety related matters.

The Health and Wellbeing Committee is responsible for promoting wellbeing activities across the organisation that support the work of the Occupational Health and Safety Committee in emotional or mental health safety.

9.2.2 External and internal context

As risk identification, assessment, and analysis is undertaken at officer level, it is undertaken from knowledge about the internal and external context for that officer's role and team's operations.

9.2.3 Defining risk criteria

The Standard states: "the organisation should specify the amount and type of risk that it may or may not take, relative to objectives.[13]"

Council's Risk Management Policy documents likelihood and consequence criteria for assessing Council's risks. The consequence criteria are set with consideration of Council's not-for-profit environment, and have been informed by *Standards Australia Limited/Standards New Zealand,*

[12] Standards Australia Limited, *ISO Australian Standard 31000:2018 Risk Management – Guidelines,* p9

[13] Standards Australia Limited, *ISO Australian Standard 31000:2018 Risk Management – Guidelines,* p10

HB266:2010 Guide for managing risk in not-for-profit organizations and includes a number of consequence types that Council must consider.

9.3 Risk assessment

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation, each of which are detailed below.

Risk assessments are conducted systematically and collaboratively, with input from key stakeholders and using the best available information and further investigation as required.

9.3.1 Risk identification

The purpose of risk identification is to find and describe risks that may prevent Council achieving its objectives, and should consider:

- what events could prevent achievement of objectives and how impactful they are on this
- vulnerabilities in systems and processes that need to be addressed
- changes in the external and internal context that may be creating emerging risks.

Council has a number of forums and processes for identifying risks, which include:

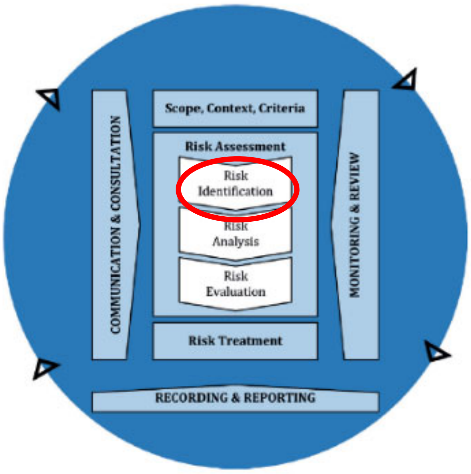


Figure 4 — Process

Forum	Details
Communication and awareness	Notification by staff to their manager or the Manager Governance of a potential or actual risk which results, or may result in an incident report
	Notification by community members to Council of a potential or actual risk which results, or may result in an incident report
Meeting structure	Department based team meetings, including tool box meetings for outdoor staff
	Maternal and child health staff in-service meetings
	Occupational Health and Safety Committee meetings
	Health and Wellbeing Committee meetings
	Management Executive Group and Loddon Leaders meetings
	Audit and Risk Committee meetings
	All staff meetings
Event	Incidents, accidents and near misses that happen in the workplace or in the community environment that are reported to Council and investigated for root cause
Audits	Internal audit program, which is a risk based program focusing on new or emerging risks, identified on an annual basis, with scope to change priorities if needed
	Insurance audits
	WorkSafe audits
	External (financial) audits
Processes	Requirement for contractors to meet minimum compliance standards prior to being engaged
	Workplace inspections which are undertaken twice per year
	Business impact analysis from the Business Continuity Plan which are undertaken; one directorate per quarter
Documentation	Registers for hazardous substances which are reviewed periodically

The product from risk identification is a risk statement. A good risk statement incorporates the following elements:

CAUSE (EVENT) → **RISK** → **IMPACT**

Example:

The requirement by Council to limit annual rates increases under the Fair Go Rates System parameters (Cause) limits Council's ability to raise rating revenue annually (Risk) which may result in Council becoming financial unsustainability over time (Impact).

Consideration of each element above will ensure risk statements are sufficiently clear for others to understand.

9.3.2 Risk analysis

The purpose of risk analysis is to understand the nature of the risk, the likelihood of it happening, the consequence of it happening, and whether we have any mitigating controls in place to reduce the risk.

This process enables each of the identified risks to be consistently rated so that the relative priority of risk treatments can be determined.

Informal risk analysis is undertaken daily by officers during their work, much of the time without even thinking of it. An example of this is wiping water off the kitchen floor so no one slips on it.

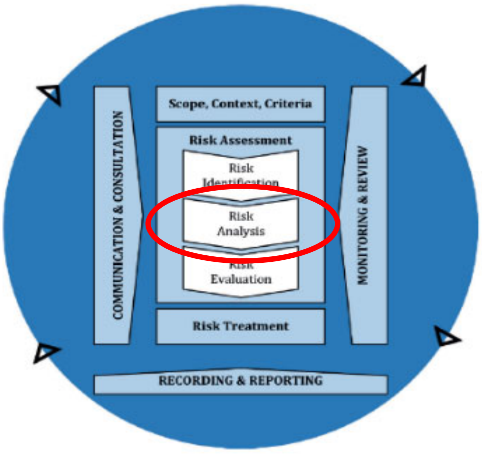


Figure 4 — Process

Formal risk analysis is undertaken with a software program (Reliansys Risk Module) that records the risk, and where analysis of the risk is undertaken. It is a three step approach (as per below), and inputs into this program create risk registers.

1. Inherent risk:
Likelihood and consequence analysis
= Inherent risk rating

→

2. Controls:
- Identification of controls
- Assessment of effectiveness of controls in reducing risk

→

3. Residual risk:
Likelihood and consequence analysis
= Residual risk rating

9.3.2.1 Inherent risk

Inherent risk is the risk assessment undertaken without considering any controls. It is an important first step in analysing the risk to understand the whole impact of the risk should controls not be effective, or fail. This is an analysis of worst-case scenario.

9.3.2.2 Current controls

A control is a measure or action that modifies or regulates risk. The goal is to modify the risk down to a lower rating. Controls include policies, procedures, work practices and processes, technology, just to name a few.

Controls can be:

1. Preventive: a control that prevents a risk from occurring
2. Detective: a control that detects risks prior to them occurring or while they are in motion
3. Corrective: controls that are put in place after a risk event occurs to reduce the impact of the risk.
4. Reactive: a control that is put in place after an risk event

The effectiveness of controls is an important consideration when analysing risk, and Council's software program provides guidance on how to assess controls.

9.3.2.3 Residual risk

The residual risk is the amount of risk that remains after controls are documented, and represents the risk in its current state. It is important that the risk analysis is undertaken over time on each risk to understand whether the residual risk remains, and whether it sits within risk appetite.

In order to undertake risk analysis the Risk Management Policy must be referenced, as it has the Consequence Criteria (in Appendix A) and the Likelihood Criteria (in Appendix B).

In addition to this, the Risk Management Procedure will assist risk owners in the analysis and use of RelianSys Risk Module.

9.3.3 <u>Risk evaluation</u>

The purpose of risk evaluation is to compare the risk analysis results against Council's risk appetite to determine where additional action is needed. The ideal scenario is to implement controls to a risk level that is acceptable to Council (i.e. within the risk appetite) with surety that the controls are effective.

If this does not happen, possible decisions include:

- do nothing
- further investigate to better understand the risk
- maintain existing controls
- increase controls
- reconsider strategic objectives
- consider risk treatment options.

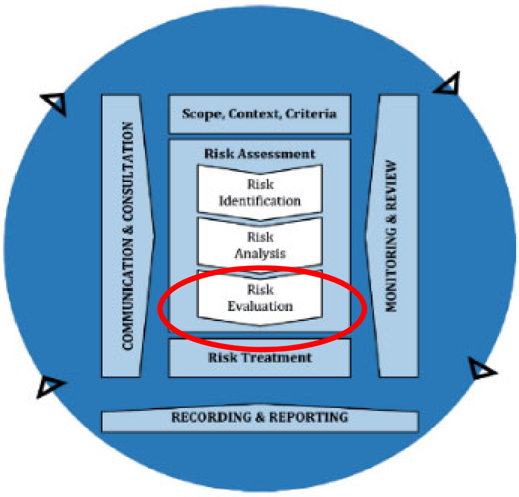


Figure 4 — Process

Any risks that have a residual risk rating of Very High (unconditional) and High (conditional) must have treatments identified and implemented with the objective of improving the control environment and reducing the likelihood, consequence, or both.

9.4 Risk treatment

9.4.1 <u>Selection of risk treatment options</u>

Risk treatments are designed to minimise the risk. Deciding on the most appropriate risk treatment will be undertaken by "balancing the potential benefits derived in relation to the achievement of the objectives against costs, effort or disadvantages of implementation."[14]

Risk treatment involves an iterative process of:

- formulating and selecting risk treatments
- planning and implementing risk treatments
- assessing effectiveness of risk treatments
- deciding whether the resulting residual risk is acceptable
- taking further treatment actions if the residual risk is not acceptable.

[14] Standards Australia Limited, *ISO Australian Standard 31000:2018 Risk Management – Guidelines,* p10

Examples of risk treatments are:

Risk treatment	**Application of risk treatment**
Take risk	Pursue an opportunity that falls within Council's risk appetite
Remove risk source	Remove whatever is creating the risk for Council
Change likelihood or consequence	• Train staff in procedures • Test procedures to ensure they are sound • Implement monitoring and control program, e.g. Fraud and Corruption Control Plan • Implement a strong governance framework for policies and procedures • Corrective actions resulting from incident reports • Implement Business Continuity Plan • Implement Disaster Recovery Plan (for IT) • Regularly review instruments of delegation of powers, duties and function • Risk-based internal audit program
Share the risk	Transfer part or all of the risk through insurance contracts, outsourcing the risk through commercial contracts, partnerships, etc.
Avoid the risk	Decide not to start or continue with the activity that gives rise to the risk
Retain the risk	Accept the risk by choice as the risk falls within the Council's risk appetite

9.4.2 Preparing and implementing risk treatment plans

Risk treatment plans provide documentation of corporate assumptions and actions, which helps during reassessment of risks in identifying the rationale for why a risk treatment was selected.

A risk mature organisation will implement risk treatment plans where required following risk evaluation. Council has not previously implemented risk treatment plans, but this will be a continuous improvement activity embedded through the work of Loddon Leaders.

9.5 Monitoring and review

In addition to being an important continuous improvement activity, monitoring and review of the risk registers ensures that risk assessments and risk treatments are current for the objectives of the Council.

Monitoring will be incorporated into reporting cycles as follows:

- Council will monitor strategic risks every six months.
- The Audit and Risk Committee will monitor strategic and operational risks every quarter, with strategic risks provided in quarter 1 and 3 and operational risks provided in quarter 2 and 4.
- Loddon Leaders will monitor operational risks.
- The Occupational Health and Safety Committee will monitor safety risks, which includes assessment of near misses, hazards, and safety incidents.
- The Management Executive Group, project managers and project officers will monitor project risks throughout the life of a project.
- All risk owners will monitor their specific risks, and escalate them through the appropriate channels when they are outside of risk appetite.

Reporting of risks is covered in the next section of this framework; however, between reporting cycles, risks should be monitored and must be escalated where a risk rating is increased through the review.

Strategic risks and project risks are subject to specific monitoring and review outside this framework.

The following are the monitoring and review parameters for escalation of **operational risks**:

Residual risk level	Risk acceptance	Recommended management response	Timeframe	Responsibility
Very high	**Unacceptable region: Action required:** Risk can only be allowed to continue under exceptional circumstances and with the approval of CEO.	Immediate notification to the CEO	Immediate	Relevant director
		Risk activity is to cease unless the CEO agrees that it can continue; however, risk treatment plans must be implemented as a priority	Interim action within 7 days	Risk owner with support from relevant manager
			Detailed risk treatment plan within 14 days	Risk owner with support from relevant manager
			Weekly monitoring, or more if directed by CEO	Risk owner
		Reported to Audit and Risk Committee at next meeting		Director Corporate with support from risk owner
High	**Tolerable region: Monitoring required**: Risk mitigation efforts must increase to reduce the risk as far as reasonably practicable, unless cost significantly outweighs the benefit or reduction is impracticable.	Immediate notification to relevant director	Immediate	Relevant manager
		Risk monitored, and if the threat remains after 14 days, a risk treatment plan must be developed and implemented	Interim action within 14 days	Risk owner with support from relevant manager
			Detailed risk treatment plan within 30 days	Risk owner with support from relevant manager
			Fortnightly monitoring, or more if directed by relevant director	Risk owner
		Reported to Audit and Risk Committee at next meeting		Director Corporate with support from risk owner
Medium	**Tolerable region: Monitoring required**: Confirm risk mitigation efforts are effective in reducing the risk as far as reasonably practicable.	Risk monitored	Quarterly	Risk owner
		Continue to manage as part of ongoing operations		Risk owner
		Review quarterly, or if anything changes within the quarter		Risk owner

Residual risk level	Risk acceptance	Recommended management response	Timeframe	Responsibility
Low	**Acceptable region:** **No action required:** No further risk reduction actions are required	Risk monitored	Annually	Risk owner
		Continue to manage as part of ongoing operations		Risk owner
		Review annually, or if anything changes within the year		Risk owner

9.6 Recording and reporting

The risk management process and its outcomes are recorded in a strategic risk register, project risk registers, a fraud risk register and various operational risk registers.

The purpose of recording and reporting is to:

- provide an enterprise-wide risk profile to the Management Executive Group, Audit and Risk Committee and Council
- understand whether the risk profile is within Council's risk appetite
- drive best practice in risk management which will improve performance management
- provide good information to inform decision-making.

The governance framework for risk management ensures that reporting is provided to Council through the committee structure that includes the Health and Safety Committee, Loddon Leaders and the Audit and Risk Committee, and this has been documented earlier in this framework. The following is the reporting cycle for risk management:

Reporting to	Minimum review frequency	Reporting by	Authorising and reporting mechanism
Strategic risk			
Council	Six-monthly, as per Local Government Act 2020 and Local Government Performance Reporting Framework	Audit and Risk Committee (through the Director Corporate)	*For approval*: Detailed report of “strategic risks to Council's operations, their likelihood and consequences of occurring and risk minimisation strategies“
	As required if Council changes strategic direction	Audit and Risk Committee (through the Director Corporate)	*For approval*: Detailed report around change in strategic direction and the impact on the current Strategic Risk Register
Audit and Risk Committee	Six-monthly, as per Local Government Act 2020 and Local Government Performance Reporting Framework	Director Corporate	*For endorsing*: Detailed report of “strategic risks to Council's operations, their likelihoodand consequences of occurring and risk minimisation strategies“

Reporting to	Minimum review frequency	Reporting by	Authorising and reporting mechanism
	As required if Council changes strategic direction	Director Corporate	*For endorsing*: Detailed report around change in strategic direction and the impact on the current Strategic Risk Register
Project risk			
Management Executive Group	Report following completion of each project phase	Project managers	*For monitoring*: Detailed report about key projects and their risk status: financial, time, stakeholder, etc.
Operational risk			
Council	Six monthly, as per the Local Government Act 2020	Audit and Risk Committee (through the Director Corporate)	*For approval*: Summary report through Audit and Risk Committee Biannual Report of Activities of the Committee
	As required if internal or external context changes significantly or Council changes programs or services	Audit and Risk Committee (through the Director Corporate)	*For approval*: Detailed report around change in context or services or programs and the impact on Operational Risk Registers
Audit and Risk Committee	Six-monthly (in the quarters that Strategic Risk is not provided to the Committee)	Director Corporate	*For endorsing*: • Overall risk profile • Detail of very high and high risks and any risk treatment plans in place • New and emerging risks • Detailed report of operational risks • Summary of Loddon Leaders compliance meeting
	As required if internal or external context changes significantly or Council changes programs or services	Director Corporate	*For endorsing*: Detailed report around change in context or services or programs and the impact on Operational Risk Registers

Reporting to	Minimum review frequency	Reporting by	Authorising and reporting mechanism
Loddon Leaders (Compliance meeting)	Quarterly report	Manager Governance	*For monitoring*: • New and emerging risks • Detail of very high and high risks and any risk treatment plans in place • Sample assessment of risks across directorates • Summary of OH&S Committee Meeting
Occupational Health and Safety (OH&S) Committee	Quarterly Report	Manager Governance	*For monitoring and action:* • Details of hazards, near misses, and incidents • Details of risk mitigation activities
Management Executive Group	Quarterly report	Director Corporate	*For monitoring:* • New and emerging risks • Risk profile and changes to the profile from the previous quarter • Detail of very high and high risks and any risk treatment plans in place

10 ROLES AND RESPONSIBILITIES

Risk management is an integral part of an organisation's governance structure, and exists to ensure that the organisation achieves its objectives. It is therefore, aligned to performance management. ***Every member of the organisation has a responsibility to manage risk***.

10.1 Council

Although risk management is a day-to-day responsibility of management, as the most senior authority, risk management is the ultimate responsibility of Council. Council delegates via the Act oversight responsibility for risk management to the Audit and Risk Committee.

The reporting structure ensures that Council is provided with regular reports on risk management via the Audit and Risk Committee Report, presented to Council following each Audit and Risk Committee Meeting.

Under Section 9(2)(c) of the Act, Council must give effect to the overarching governance principles in the performance of its role, which includes: "the economic, social and environmental sustainability of the municipal district, including mitigation and planning for climate change risks, is to be promoted".

The Council also considers a six-monthly report on the Committee's activities in accordance with Section 54(5) of the Act.

Under the Local Government Performance Reporting Framework, Council has the responsibility of producing six-monthly reports on strategic risks to Council's operations, their likelihood and consequence of occurring, and risk minimisation strategies.

In addition to the above, Council's responsibilities are to:

- perform its role as a Council and makes decisions in the context of risk
- review and approve the Risk Management Policy, Risk Management Framework, and Risk Appetite Statement
- review and approve the Risk Management Implementation Plan ensuring that actions are completed and new actions identified to progress risk management maturity.

10.2 Audit and Risk Committee

Council has established an Audit and Risk Committee pursuant to section 53 of the Local Government Act 2020 to support it in discharging its oversight responsibilities, including those related to risk management, reflected in the Audit and Risk Committee Charter.

The Committee meeting agendas include some aspect of risk management, including outstanding audit actions that have been identified through internal audits to mitigate risks, half yearly updates on the actions in Risk Management Implementation Plan, and sector reports from Local Government Inspectorate, Auditor-General Victoria, Ombudsman Victoria and the Independent Broad-Based Anti-Corruption Commission.

Section 54(5) of the Act states the committee must:

a) prepare a biannual audit and risk report that describes the activities of the Audit and Risk Committee and includes its findings and recommendations; and
b) provide a copy of the biannual audit and risk report to the Chief Executive Officer for tabling at the next Council meeting.

In addition to this report, a summary of Audit and Risk Committee meetings is provided to the Council at the Council Meeting following the Audit and Risk Committee Meeting.

The Audit and Risk Committee reviews and endorses risk management documents before they are presented to Council for approval.

10.3 Loddon Leaders

The Loddon Leaders Terms of Reference outlines the relevant risk management responsibilities, and as risk maturity increases, it is expected the Terms of Reference will evolve over time.

10.4 Management Executive Group

The Management Executive Group, comprising the Chief Executive Officer and three directors, are advocates of best practice risk management for the organisation. To provide them with oversight of the risk management environment, they are provided with quarterly reports around Council's risks. This ensures that they are aware of new and emerging risks and understand the status of the risk profile.

10.5 Managers

As well as having risk management responsibilities in their own right and responsibilities associated with Loddon Leaders, managers have the added responsibility of ensuring that their staff are aware of their risk management responsibilities, that they act in a safe and responsible manner, and are reporting new and emerging risks in their area of the organisation.

10.6 Director Corporate

The overarching coordination of risk management for Council lies with the Director Corporate, who has a key role in developing and reviewing risk management documentation, facilitating the Audit and Risk Committee, managing outstanding actions resulting from internal audit reviews that identify risk mitigation activities, providing advice to staff, and monitoring the effectiveness of Council's risk management software.

10.7 Manager Governance

The Manager Governance has responsibility for ensuring relevant corporate frameworks exist to support workplace safety, including management of safety hazards, near misses and incidents.

10.8 Staff, contractors and volunteers

10.8.1 Staff

The induction process for staff articulates Council's commitment to provide a safe environment for staff, the community, and travelling public. To support this commitment, every position description developed for Council staff includes a standard OH&S clause.

An induction module around general risk management is being developed to provide staff with the knowledge and expectations around risk management while working with Council.

10.8.2 Contractors

Council will not engage contractors unless they have been verified through a process that includes providing certificates of currency for insurances, and depending on the level of risk associated with their activities, evidence of safety systems.

This provides some certainty that contractors being engaged by Council have the same level of commitment to a safe working environment, particularly as many of Council's contractors work in the open around community and the travelling public.

10.8.3 Volunteers

Council engages volunteers for the delivery of a range of services to the community. Council's Volunteers' Code of Conduct, which is being developed, will contain minimum standards expected of volunteers around safe operating practices.

In addition to this, there will be a dedicated volunteer induction portal that will require new volunteers to adhere to compliance such as Working with Children Checks, Police Checks, etc.

11 DEFINITIONS OF TERMS OR ABBREVIATIONS USED

Term	Definition
Consequence	The outcome of an event affecting objectives. Objectives can be strategic objectives outlined in the Council Plan, specific project objectives, or objectives relating to standard Council operations and activities. A consequence can be certain or uncertain and can have positive or negative direct or indirect effect on objectives.[15]
Control	A measure that maintains and/or modifies risk.[16]
Inherent risk	Represents the amount of risk that exists in the absence of controls.[17]
Likelihood	The chance of something happening.[18]
Residual risk	Is the amount of risk that remains after controls are accounted for.[19]

[15] Standards Australia Limited/ Standards New Zealand, ISO 31000:2018 Australian Standard Risk Management Guidelines, p2

[16] Standards Australia Limited/ Standards New Zealand, ISO 31000:2018 Australian Standard Risk Management Guidelines, p2

[17] https://www.fairinstitute.org/blog/inherent-risk-vs.-residual-risk-explained-in-90-seconds, Accessed: 1 March 2022

[18] Standards Australia Limited/ Standards New Zealand, ISO 31000:2018 Australian Standard Risk Management Guidelines, p2

[19] https://www.fairinstitute.org/blog/inherent-risk-vs.-residual-risk-explained-in-90-seconds, Accessed: 1 March 2022

Term	Definition
Risk	The effect of uncertainty on objectives. An effect is a deviation from the expected. It can be positive, negative, or both, and can address, create or result in opportunities or threats.[20]
Risk appetite	The amount of risk the Council is willing to accept in pursuit of strategic objectives.
Risk assessment	The overall process of risk identification, analysis, and evaluation.[21]
Risk management	Coordinated activities to direct and control an organisation regarding risk.[22]

12 TRAINING

Training in risk management concepts and the risk management process will be provided for staff upon induction and refresher training. To support a commitment to this, training has been identified on the Risk Management Implementation Plan as an ongoing action.

13 REVIEW

All risk management documentation is reviewed periodically to ensure it remains current for Council activities. This framework, having had its first review, will now be reviewed as required, but no later than four years from the adoption of this version.

[20] Standards Australia Limited/ Standards New Zealand, ISO 31000:2018 Australian Standard Risk Management Guidelines, p1

[21] [21] Standards Australia Limited/ Standards New Zealand, ISO 31000:2018 Australian Standard Risk Management Guidelines, p11

[22] [22] Standards Australia Limited/ Standards New Zealand, ISO 31000:2018 Australian Standard Risk Management Guidelines, p1