Risk Management Operating Guideline

21 April 2021   *Administration*

PURPOSE

The Risk Management Operating Guideline sets the foundation for people who create and protect value in Council by managing risks, making decisions, setting and achieving objectives and improving performance.

OPERATION

Managing risk is part of good governance and leadership and is fundamental to how Council is managed at all levels. It contributes to the improvement of management systems based on the principles, framework and processes as illustrated in the below:

Principles provide guidance on the characteristics of effective and efficient risk management, communicating its values and explaining its intention and purpose.

Framework is to assist the Council in integrating risk management into activities and functions (including projects).

Process includes the risk assessment of the activity by addressing the risk identification, risk analysis and risk evaluation to identify the risk treatments to mitigate the risk.
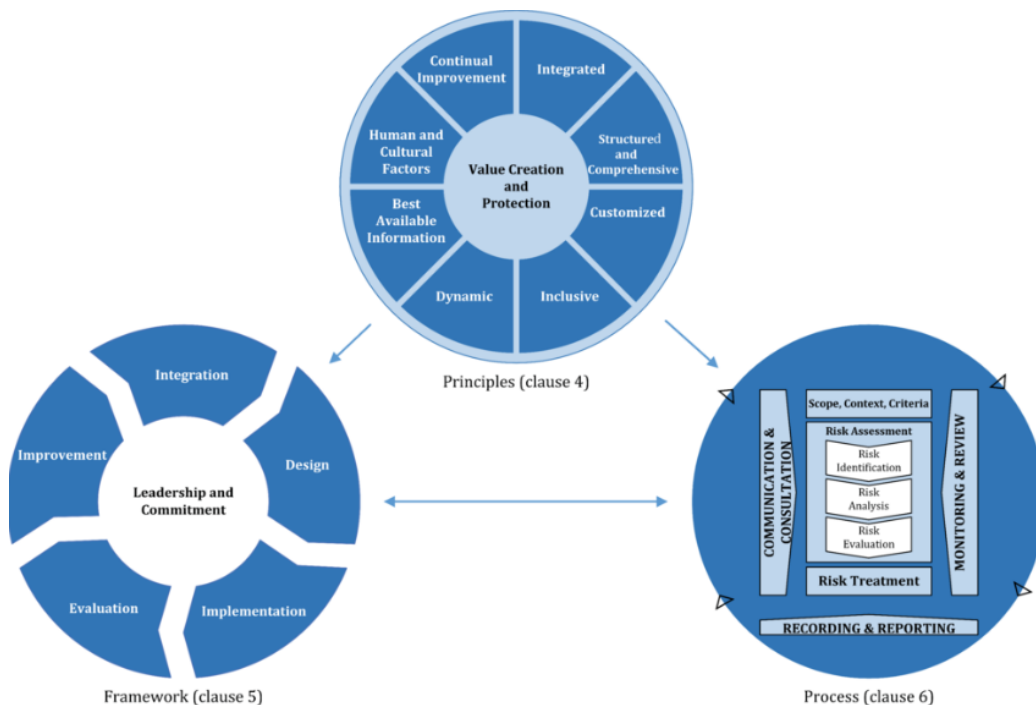
Please refer to *Related Documents Table* for a detailed image of the above.

PART 1
### ENTERPRISE RISK MANAGEMENT AND RISK APPETITE

Enterprise Risk Management includes the methods and processes used by the organisation to manage risk and maximise opportunities related to the achievement of Council's objectives. It is intended to be embedded in the organisation's culture, enabling well informed decision making within Council's risk appetite.

Risk appetite can be explained as the total impact of the risk the organisation is prepared to accept in the pursuit of achieving its strategic objectives.

Risk Appetite has two components to it:

- Risk tolerance: how much risk can the organisation choose to accept?
- Risk capacity: how much risk can the organisation afford to take?

Balancing Risk
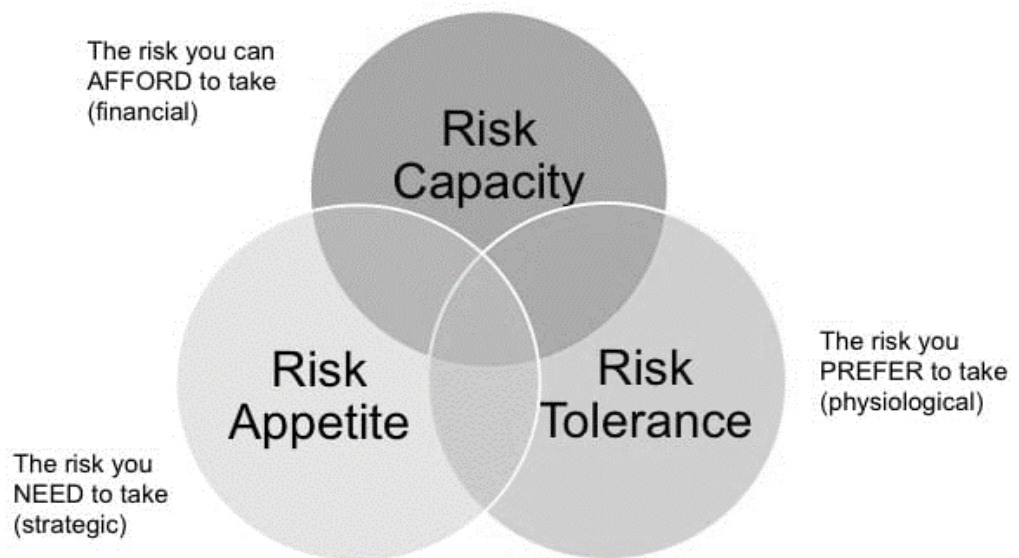
Understanding risk appetite will help the organisation in the efficient allocation of resources across all identified risks and enable the pursuit of opportunities as boundaries can be defined around opportunity seeking actions.

The risk appetite statement informs the development of risk tolerances for the CoA and provides guidance on how the risk appetite statement is to be applied in everyday business activities and decisions. Whilst the tolerance for a Local Government entity is often guided by the parameters of legislation, mere compliance does not efficiently express the total potential for risk taking and its associated tolerance; these are expressed through appropriate risk culture practices.

The CoA will accept a moderate residual risk rating however significant focus it to be put on the healthy and mature risk conversations through the executive Strategic Risk and Internal Audit group (SRIA), which underpins the organisation's risk culture and enables better informed decision making. Each relevant Executive leader has the opportunity to escalate and monitor risk concerns by bringing matters through to SRIA. This group monitors emerging strategic and reputational risks in line with the Waterline principle and philosophy.

This strategic governance structure empowers the Executive to make decisions and adjust conventional risk tolerances on a risk by risk basis.

However, as a rule of thumb, conventional enterprise risk management is assessed through the below risk appetite statements:

Extent of Risk Appetite	Risk Tolerance	Risk Management Approach
High Appetite (Open) *CoA will operate in this area or in this way after all options are considered, and the most appropriate option selected for an acceptable level or reward or value for money*	High Tolerance	Innovation / venture / explore (strategy)
Moderate Appetite (Acceptable) *CoA will operate in this area or this way after risks have been effectively mitigated in order to pursue opportunities*	Moderate / Medium tolerance	Confident
Low Appetite (Tolerable) *CoA may operate in this area or int his way where the value is assessed as worthwhile, and only after risks have been effectively mitigated or uncertainty minimised*	Limited / Low tolerance	Conservative
No Appetite (Unacceptable) *CoA will not operate in this area. No willingness to take on any risk*	Zero tolerance	Avoid

Above moderate residual risk ratings are only acceptable subject to fully informed decision making, proper reporting and continuous monitoring of risk controls.

A **zero-risk tolerance** is present for:

- Compliance and safety breaches
- Non-compliance with the Code of Conduct
- Prolonged disruption to critical business functions (as identified through the Business Continuity Plan and Service Register)
- Decisions that have no sound financial basis and have a significant negative impact on the future generations of the city community and its ratepayers.

Quality of Deliverable

There is a low appetite for risks that may result in the CoA providing poor service delivery (from a local government entity perspective), especially when poor quality service offerings could lead to an adverse impact on the City ratepayers.

Organisational Performance

The CoA has a moderate appetite for decisions in relation to the core deliverables outlined in the Strategic Plan 2021-2024 and for decisions in relation to its organisational work plan

Corporate Governance

There is a low appetite for activity that may result in non-compliance with legislation, statutory obligations and policies. The CoA has a zero tolerance for deliberate non-compliance with legal, statutory and policy requirements.

Financial

The CoA has a low appetite for decisions that could have a negative impact on the organisation's financial sustainability.

Fraud

There is a low appetite for fraud risk and zero tolerance for fraud incidents. The CoA has corporate governance measures in place to deal with a suspected maladministration and serious and/or systemic corruption. Internal Audit measures have been developed to minimise the potential for instances of fraud and corruption.

Information Communication Technology (ICT) and Information Security

The CoA has a low appetite for risk that could lead to information or data security breaches and a low appetite for system failures that could disrupt normal business. The CoA has no appetite for activities that may increase its exposure to threats on its assets arising from external malicious attacks.

Information Management

The CoA has a low appetite for activities that may compromise processes governing the use of information, its management and publication. The CoA has zero tolerance for the deliberate misuse of its information.

Work Health & Safety

The CoA has no appetite for risks to the health and safety of its workers, which cannot be eliminated or minimised so far as reasonably practicable.

PART 2

PRINCIPLES

Effective risk management requires all the elements below:

    a)   Integrated

          Risk management is an integral part of all Council operations and projects.

    b)   Structured and comprehensive

A structured and comprehensive approach to risk management contributes to successful risk identification and management including prudential reporting.

c) Customised

The risk management framework and process are created in line with Council's Strategic Plan and risk management culture.

d) Inclusive

The framework promotes an inclusive approach in the involvement of the relevant stakeholders, executive SRIA group members and management, to enable informed decision making.

e) Dynamic

Risks can emerge, change or disappear as external and internal factors develop. 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.

g) Human and cultural factors

Human behaviour and culture influence any/all aspects of risk management at an operational or project level.

The CoA encourages a safe environment where staff and volunteers are encouraged and supported to escalate risk to their leader, Manager Governance, or Corporate Governance team for further assessment.

h) Continual improvement

Risk management is continually improved through learning, experience and informing others. Risk management systems are audited by the Local Government Association Mutual Liability Scheme (the Scheme) every two years.

The Scheme will assess various aspects of council including WHS and request feedback and evidence from CoA in relation to our risk management practices. Feedback as provided by the Audit and Risk Committee is also considered and implemented.

PART 3
RISK MANAGEMENT FRAMEWORK

Leadership and commitment

CoA are committed through SRIA and Executive to ensure that risk management is integrated into all organisational activities by:

- Developing and implementing the Risk Management Operating Guideline, and supporting tools and processes;
- Allocating appropriate resources for risk management;

- Supporting and encouraging risk escalation; and assigning roles, responsibilities and accountabilities with respect to risk management and communicating these at all levels of the organisation.

<u>Roles and Responsibilities</u>

Roles and responsibilities ensure a transparent approach to managing risk within Council.

Roles	Responsibilities
Council	Note the Risk Management Operating Guidelines
Audit & Risk Committee	Review and note the Risk Management Operating Guidelines in accordance with its Terms of Reference
Strategic Risk & Internal Audit Group	Review and endorse the Risk Management Operating Guidelines Ensure the guideline is implemented and delivers a consistent approach to risk management by assigning responsibility and accountability at appropriate levels within the organisation Be a forum for risk escalation Monitor Council's overall risk profile and mitigation strategies.
Chief Executive Officer	Promote a strong risk management culture by providing firm and visible support for risk management including ensuring appropriate accountability for the management of risk. Ensure that appropriate resources are allocated to managing risks. Ensure that the Leadership Team have the necessary knowledge and skills to effectively fulfil their risk management responsibilities and are accountable for risks arising from the activities of their programs.
Executive, Associate Directors and Managers	Commitment to, and promotion of, the Risk Management Operating Guideline Ensure that risk management is embedded into all critical functions and activities. Empower staff to actively be involved in managing risk. Promote a proactive risk culture and encourage risk escalation. Review Council's Strategic Risks.

Corporate Governance	Provide guidance and assistance to all staff in relation to the application of this operating guideline.
	Ensure relevant risk information is reported and escalated to SRIA or Audit & Risk Committee or cascaded to staff, as relevant.
	Maintain the Risk Management Operating Guideline
	Maintain the Risk Registers that are reported to SRIA and timeframes as required.
	Provide support and advice to Leadership and staff in the application and use of the Risk Management Operating Guideline.
Employees, Volunteers & Contractors	Understand the risk management processes that are integrated into all Council activities
	Identify, evaluate, report and manage risks in their daily activities and projects.

Implementation

Council's risk management philosophy is implemented through induction, leader training is captured through the Network Access Form, proactive risk awareness sessions and the facilitation of risk awareness workshops. The CoA risk culture continues to build through more conversations regarding risk and opportunity management.

Proactive risk management sessions, facilitated by Corporate Governance are held every six months with Managers across CoA to discuss current SRIA items raised, operational risks and identify new and upcoming projects to ensure a risk overview is considered.

Through formal advice from the Audit & Risk Committee, Council Members have a practical understanding of Council's Risk Management Operating Guideline. Council members make informed decisions based on sound risk management principles. Council Members note the activities of the Audit & Risk Committee and risk implications on recommended decisions are incorporated in every Council report as part of a mandatory heading in the reporting template.

Evaluation

Council will undertake periodic reviews of the risk management resources. Every two years CoA will be audited by the Scheme on risk management systems.

Improvement

To maintain and improve the value of risk management to the organisation, Council will monitor and adapt its Risk Management Operating Guideline, with a view to continually improve the suitability, adequacy and effectiveness of the risk management process.

PART 4
RISK MANAGEMENT PROCESS

The Risk Management process needs to be dynamic and tailored to ensure outcomes are met. The CoA have a number of tools and resources available via the OSCAR page for

assistance in the risk management process and these tools are made available to all employees, volunteers and contractors. The Risk page on OSCAR contains the following tools: Risk Rating Table, Generic Risk Register, Construction Works Generic Risk Register, Simplified Risk Register & Events Risk Management Plan.

Communication and consultation

The purpose of communication and consultation is to assist relevant stakeholders in understanding risk, the basis on which decisions are made and the reasons why particular actions are required. Communication and consultation with appropriate external and internal stakeholders should take place within and throughout all steps of the risk management process.

Scope, context, and criteria

The purpose of establishing the scope, the context and criteria is to enable effective risk assessment and appropriate risk treatment. The goals, objectives, strategies, scope and parameters of the activity, or part of the Council organisation to which the risk management process is being applied will be defined.

-

Risk assessment

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation. The aim of risk identification is to develop an inclusive list of events that may occur which, if they do, are likely to have an impact on the achievement of Council's objectives.

Understanding the nature of the risk and its characteristics, including the level of risk assists in the evaluation of the risk. Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required.

Risk treatment

The purpose of risk treatment is to select and implement options for addressing risks.

Acceptance – not recognising the risk or conscious decision to accept the risk

Avoidance – not proceeding with project or idea

Control – reduce likelihood, limit consequences (impact)

Transfer – shifting responsibility of risks and losses to another party through legislation or contract (eg. Indemnity or insurance policy)

Monitoring and review

. Ongoing monitoring and review should take place in all stages of the process and include planning, gathering and analysing information, recording results and providing feedback.

Recording and reporting

The risk management process and its outcomes should be documented using CoA risk registers and reported through appropriate mechanisms (if required) such as SRIA and leadership.

EFFECTIVENESS OF RISK CONTROLS

A control can be defined as an existing process, policy, device, practice or other action that acts to minimise or eliminate negative risk or enhance positive opportunities. The effectiveness of controls can be rated as either:

- **Satisfactory:** The control environment is considered to be operating effectively and thought to be providing an adequate level of assurance that risks are being mitigated and opportunities are being maximised.
- **Some weaknesses**: The control environment has some weaknesses/inefficiencies. Although these are not considered to present a serious risk exposure, improvements are required to provide adequate assistance that objectives will be achieved.
- **Weak**: The control environment is not at an acceptable standard, as many weaknesses/inefficiencies exist. Adequate assurance does not exist that objectives will be achieved.

THE WATERLINE PRINCIPLE

Bill Gore articulated a helpful concept for decision-making and risk-taking, what he called the **"waterline"** principle. Think of being on a ship and imagine that any decision gone badly will blow a hole in the side of the ship. If you blow a hole above the waterline (where the ship won't take on water and possibly sink), you can patch the hole, learn from the experience, and sail on to your destination (deliver your strategic objectives). But if you blow a hole below the waterline, you can find yourself facing gushers of water pouring in, pulling you toward the ocean floor. And if it's a big enough hole, you might go down really fast. You will not arrive at your destination; you will not be able to deliver your strategic objective.

Below the waterline risks are what we call strategic risks. They need immediate escalation to the Executive.

Above the waterline risks are what we call operational risks. They can be managed at the operational level.

The biggest risk of all is taking no risk at all. Calculated risks provide opportunities for the organisation to grow; however, they are conscious to avoid taking risk that could blow holes below the waterline.

It's important to note that some operational risks may develop into strategic risks. It's critical to identify these emerging risks timely. They need to be monitored closely.

above the waterline   below the waterline

Adapted from Gore Pty Ltd
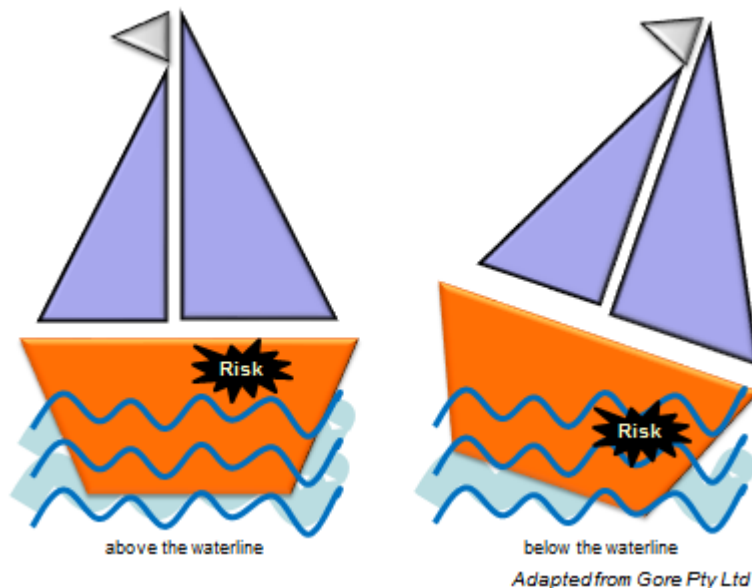
INSURANCE

Council's insurance portfolio is administered by the Corporate Governance team.

As an insured, Council has the obligation to notify its insurers of any substantial increase of risk exposure covered by the insurance cover. Examples are: fire protection system being switched off for repairs or maintenance, long term building vacancy, new Council activities or events outside normal council business activities etc. It is important to notify the Corporate Governance team at your earliest convenience. This will help the team to lodge accurate and up to date information to Council's insurers.

The Corporate Governance team also needs to be notified of any insurance requirements where there is an insurable interest or a potential liability exposure, or in the event of changes impacting an existing insurance cover. Examples are: new assets (new cover required), disposal of assets (insurance cover cancellation), etc.

INDEMNITIES, CAPPED LIABILITIES, HOLD HARMLESS AGREEMENTS

Council may in some cases grant some contractual indemnities to third parties. These decisions need to be based on sound risk management as Council may potentially be exposed to some significant risks. Any variations to Council's standard contract templates need to be properly risk assessed. The Corporate Governance team must be consulted in this

assessment and will be able to assist in the risk assessment and the negotiation around the amended indemnity wording.

PRUDENTIAL REPORTING

Please refer to section 48 of the *Local Government Act 1999*.

The Council Report required under this section needs to include an assessment of any risks associated with the project and the steps that can be taken to manage, reduce or eliminate those risks. Please refer to the Prudential Reporting Policy owned by finance and consult with the Corporate Governance team for assistance in preparing a risk assessment.

INTERNAL CONTROLS

Council's Internal Controls are processes for assuring Council's achievement of objectives in operational effectiveness and efficiency, reliable financial reporting, and compliance with laws, regulations and policies. The Internal Control Systems are the policies and procedures that help ensure appropriate risk responses are executed and include a range of activities such as approvals, delegations, security of assets and segregation of duties.

Internal Controls play an important role in detecting and preventing fraud and protecting the organisation's resources, both physical (eg. machinery and property) and intangible (eg. reputation or intellectual property such as trademarks).

The objectives of internal controls are to ensure that public resources are adequately managed, and all employees of CoA are responsible for ensuring those controls are established, documented, maintained and adhered to across the CoA.

The Process Manager (formerly Promapp) software system is the tool to track and process map Council's internal controls.

Internal Controls Roles and Responsibilities

The Chief Executive Officer and principal member of Council must sign the financial statements in regard to internal controls as required by the *Local Government (Financial Management) Regulations 2011*.

Management must adopt a risk management approach to identifying and assessing risks and apply cost/benefit analysis in the development of internal controls. Council employees must conduct their duties in accordance with internal control processes and practices of Council.

Lines of Defence
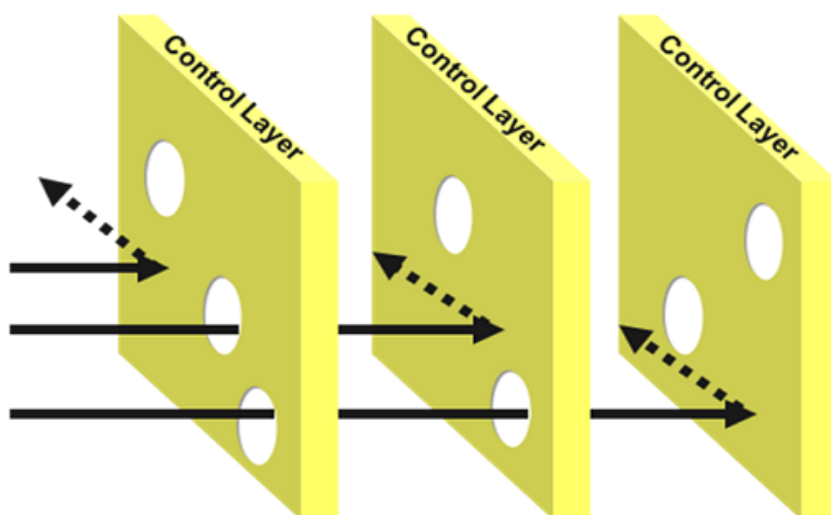
PART 5

AUDIT & RISK COMMITTEE AND STRATEGIC RISK & INTERNAL AUDIT GROUP

Strategic Risk & Internal Audit Group

The success of the Risk Management model is a result of a strong Executive involvement through monthly reporting of risk and audit matters to the Strategic Risk and Internal Audit Group (SRIA), and quarterly reporting to the Audit & Risk Committee.

SRIA has an oversight on emerging issues and strategic risks, enabling well informed decision making. The role of the group is to:

- Develop and oversee Risk Management in its practical application within the Corporation
- Ensure early, quick and clear escalation of strategic risks and emerging issues to key decision makers
- Ensure appropriate controls are in place to actively manage and monitor strategic risks and emerging issues
- Ensure that sufficiently mitigated matters return to routine operations management
- Identify and communicate key learnings and ensure that relevant processes are reviewed for continuous improvement
- When a risk has been identified, this should be escalated to SRIA to discuss and place it on a risk register so it can be monitored.

For further information please see SRIA Terms of Reference

Audit & Risk Committee

The Audit & Risk Committee is a formally appointed committee of the CoA, pursuant to Section 41 of the *Local Government Act 1999 (SA)* and operates in accordance with section 126 of the Act and its terms of reference.

The Audit & Risk Committee's role is to report to Council and provide appropriate advice and recommendations on matters relevant to its Terms of Reference in order to facilitate

decision making by the Committee and Council in relation to the discharge of its responsibilities.

For further information please see Audit Committee Terms of Reference

----

OTHER USEFUL DOCUMENTS

Related documents
- ISO 31000:2018 – International Standard Risk Management Guidelines
- Risk Rating Table (ACC2017/104073)
- Generic Risk Register (ACC2017/40158)
- Construction Works Generic Risk Register (ACC2017/40150)
- Simplified Risk Register (ACC2017/40151) for quick risk assessments on ideas or minor decisions or initiatives
- Events Risk Management Plans (ACC2017/104076)
- SRIA Terms of Reference (ACC2022/46690)
- Audit & Risk Committee Terms of Reference (ACC2021/154791)

Relevant legislation
- Local Government Act 1999 (SA)
- Work Health and Safety Act 2012
- Return to Work SA Code of Conduct for Self-Insured Employers Version 12
- Civil Liabilities Act 1936

GLOSSARY

Throughout this document, the below terms have been used and are defined as:

Risk: effect of uncertainty on objectives

Risk Management: coordinated activities to direct and control an organisation with regard to risk

Stakeholder: person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity

Event: occurrence or change of a particular set of circumstances

Consequence: outcome of an event affecting objectives

Likelihood: chance of something happening

Control: measure that maintains and/or modifies risk

ADMINISTRATIVE

As part of Council's commitment to deliver the City of Adelaide Strategic Plan, services to the community and the provision of transparent information, all policy documents are

reviewed as per legislative requirements or when there is no such provision a risk assessment approach is taken to guide the review timeframe.

This Operating Guideline document will be reviewed every two years unless legislative or operational change occurs beforehand. The next review is required in **April 2025**.

Review history:

Trim Reference	Authorising Body	Date/ Decision ID	Description of Edits
ACC2018/196182	SRIA and Audit Committee	13/09/2018	Amendments to incorporate the new ISO31000:2018
ACC2020/109550	SRIA and Audit Committee	21/04/2021	Amendments to the risk appetite statement
ACC2022/19593	CEO	21/04/2021	Amendments to the training section
TBC	SRIA and Audit & Risk Committee		Streamline document with consistent wording

contact:
For further information contact the Corporate Governance team

City of Adelaide
25 Pirie ST, Adelaide, SA
GPO Box 2252 ADELAIDE SA 5001
+61 8 8203 7203
city@cityofadelaide.com.au