Risk & Opportunity Management Policy

Objective

Seek to:

- ensure that as far as reasonably practicable, City of Albany (the City) operations do not place people, property, or the environment at unacceptable levels of risk or harm;
- add value to all the activities of the City;
- assist in achieving the Council's goals and deliver programs and services within a tolerable level of risk;
- embed risk and opportunity management into all management activities, critical business systems and processes; and
- ensure all risks are consistently assessed and managed within the City's Risk & Opportunity Management Framework.

Scope (Roles & Responsibility)

Risk Management falls on all levels of the organisation, which includes the Council as the governing body, the Chief Executive Officer and members of the Executive, staff and persons who perform functions and/or deliver services on behalf of the City.

All persons are responsible for:

- ensuring risk management action results in a movement from an endurable (negative) risk treatment towards a pleasing (positive) risk treatment;
- applying risk management practices in their area of work;
- ensuring effective communication of risk to others;
- that other persons (stakeholders) are aware of identified risks associated risk management and mitigation plans; and
- escalating risk where necessary.

Policy Statements

A: Council recognises that risk management is an integral part of all Council activities.

B: Council is committed to effective risk and opportunity management to:

- improve its ability to deliver community priorities, service delivery and outcomes for the City;
- maximise opportunities and minimise the impact and likelihood of risk;
- protect its employees, assets, liabilities, and its community by avoiding or mitigating losses; and
- provide greater certainty for our employees, residents, stakeholders, and the community in which we operate by understanding and managing our risks.

C: Council's commitment is demonstrated by:

- adopting a strategic, consistent, and structured approach to risk management;
- clearing articulating its expectation that an appropriate balance between realising opportunities and mitigating losses be demonstrated; and
- upholding the International Standard on Risk Management (ISO 31000) which provides the overall framework for risk management.

Assigned Responsibility:

- **Council**, as the governing body of the City is responsible for determining the City's risk tolerance and commitment to risk management.
- The **Audit & Risk Committee**, working with the Executive Management Team is responsible for providing compliance oversight.
- The **Chief Executive Officer, Executive** and **designated persons** are accountable for the implementation and maintenance of risk management policies and processes across the organisation.
- Persons with assigned responsibility (i.e., **Risk Owners**) are ultimately responsible for ensuring that strategic and operational risks are regularly reviewed.

Under delegation from the Chief Executive Officer:

- The **Executive Management Team** (EMT) is accountable for ensuring risk management processes are embedded into their directorate work practices and **Risk Ownership** assigned. This includes ensuring that risks are identified, managed, reviewed, recorded and acceptable risk treatments are monitored.
- **All persons** (which includes staff, contractors, and volunteers) are responsible for the implementation of risk management processes within their particular areas of responsibility.
- The **Governance & Risk Team, working with the People & Culture Team** is responsible for enabling the Executive through the provision of consultation and training resources.

Monitoring, evaluation and review

Risk assessment will be guided by the risk management processes detailed in the Standard.

The Risk & Opportunity Framework informs how risk is managed at the City of Albany.

Internal Auditing. An annual internal auditing program is to be established which will test the controls set in place by each directorate and be assessed against the key performance indictors set by the Executive and reported to Council.

External Auditing. Any external auditing will be undertaken routinely, in accordance with the *Local Government (Financial Management) Regulations 1996*.

Training and continuous improvement

Education and further professional development in the areas of risk management will be supported.

All staff who perform functions or deliver services on behalf of the City are expected to:

- attend risk & opportunity management induction;
- attend regular refresher training; and
- participate and contribute to the outcomes of training.

Consultation and Communication

Effective and open communication and consultation with internal and external stakeholders during all stages of the risk management process is crucial, as each stakeholder will have a varying perception of risk and their decisions will be based on this.

All staff of the City are to ensure stakeholders impacted by decisions have had sufficient chance to comment and provide feedback prior to implementation.

Legislative and Strategic Context

There is no legislative provision that specifically requires Councils to implement risk management.

However, there are references within the Local Government Act 1995 ("the Act") that require Councils to adopt appropriate policies, practices and procedures that ensure their assets are protected through sound administrative management.

In addition, each Council's Audit Committee is responsible for 'reviewing the adequacy of accounting, internal control, reporting and other financial management systems and practices of the Council on a regular basis.

Specifically, under Regulation 17 of the Local Government (Audit) Regulations 1996 it is a responsibility of the Audit & Risk Committee to receive the CEO reviews conducted on the appropriateness of systems and procedures in relation to risk management, internal control and legislative compliance.

Strategic Context

This policy relates to the following elements of the City of Albany Strategic Community Plan or Corporate Business Plan informing plans or strategies:

- **Pillar:** Leadership.
- **Outcome:** Strong workplace culture and performance.

Review Position and Date

This policy and procedure is to be reviewed by the document owner every two years.

Associated Documents

Documents that have a bearing on this policy and that may be useful reference material for users of this policy, follow:

- Risk Management Standard: AS/ISO 31000:2018
- Risk & Opportunity Management Framework
- Risk Management Handbook
- Health & Safety Manual
- Worksafe Resources:
    - WHS Act and Regulations
    - Codes and Guidance Material

Definitions

Key terms and acronyms used and that apply to this policy position and subsidiary supporting documents (i.e., directives, guidelines, procedures, processes etc.) and their definitions:

Term	Meaning
Communication and consultation	Communication and consultation is a dialogue between an organisation and its stakeholders. This dialogue is both continual and iterative. It is a two-way process that involves both sharing and receiving information about the management of risk. However, this is not joint decision making. Once communication and consultation is finished, decisions are made and directions are set by the organisation, not by stakeholders. Discussions could be about risks, their nature, form, likelihood, and significance, as well as whether or not risks are acceptable or should be treated, and what treatment options should be
Consequence	A consequence is the outcome of an event and has an effect on objectives. A single event can generate a range of consequences which can have both positive and negative effects on objectives. Initial consequences can also escalate through cascading and cumulative effects.
Context	To establish the context means to define the external and internal parameters that organisations must consider when they manage risk. An organisation's external context includes its external stakeholders, its local, national, and international environment, as well as any external factors that influence its objectives. An organisation's internal context includes its internal stakeholders, its approach to governance, its contractual relationships, and its capabilities, culture, and standards.
Control	A control is any measure or action that modifies or regulates risk. Controls include any policy, procedure, practice, process, technology, technique, method, or device that modifies or regulates risk. Risk treatments become controls or modify existing controls once they are implemented.
Event	An event could be one occurrence, several occurrences, or even a non-occurrence (when something doesn't actually happen that should have happened). It can also be a change in circumstances. Events always have causes and usually have consequences. Events without consequences are referred to as near-misses, near-hits, close-calls, or incidents.
External context	An organisation's external context includes all of the external environmental parameters and factors that influence how it manages risk and how it tries to achieve its objectives. It includes its external stakeholders, its local, national, and international environment, as well as key drivers and important trends that influence its objectives. It also includes stakeholder values, perceptions, and relationships, as well as its social, cultural, political, legal, regulatory, technological, economic, natural, and competitive environment.
Internal context	An organisation's internal context includes all of the internal environmental parameters and factors that influence how it manages risk and tries to achieve objectives. It includes its internal stakeholders, its approach to governance, its contractual relationships, and its capabilities, culture, and standards. Governance includes the organisation's structure, policies, objectives, roles, accountabilities, and decision-making process, and capabilities include its knowledge and human, technological, capital, and systemic resources.

Level of risk	The level of risk is its magnitude. It is estimated by considering and combining consequences and likelihoods. A level of risk can be assigned to a single risk or to a combination of risks. Common level of risk categories includes the following: extreme risk, high risk, moderate risk, and low risk. Of course, you need to define each category so that everyone is using the same terminology in the same way.
Likelihood	Likelihood is the chance that something might happen. Likelihood can be defined, determined, or measured objectively or subjectively and can be expressed either qualitatively or quantitatively (using mathematics).
Monitoring	To monitor means to supervise and to continually check and critically observe. It means to determine the current status and to assess whether or not required or expected performance levels are being achieved.
Residual risk	Residual risk is the risk left over after you've implemented a risk treatment option. It's the risk remaining after you've reduced the risk, removed the source of the risk, modified the consequences, changed the probabilities, transferred the risk, or retained the risk.
Review	A review is an activity. Review activities are carried out in order to determine whether something is a suitable, adequate, and effective way of achieving established objectives. In general, ISO 31000 2018 expects you to review your risk management framework and your risk management process. It specifically expects you to review your risk management policy and plans as well as your risks, risk criteria, risk treatments, risk management controls, residual risks, and your risk assessment process.
Risk	According to ISO 31000, risk is the "effect of uncertainty on objectives" and an effect is a positive or negative deviation from what is expected. The following will explain what this means. ISO 31000 recognizes that all of us operate in an uncertain world. Whenever we try to achieve an objective, there's always the chance that things will not go according to plan. Every step has an element of risk that needs to be managed and every outcome is uncertain. Whenever we try to achieve an objective, we don't always get the results we expect. Sometimes we get positive results and sometimes we get negative results and occasionally we get both. The traditional definition of risk combines three elements: it starts with a potential event and then combines its probability with its potential severity. A high-risk event would have a high likelihood of occurring and a severe impact if it actually occurred. While ISO 31000 defines risk in a new and unusual way, the old and the new definitions are largely compatible. Both definitions talk about the same phenomena but from two different perspectives. ISO thinks of risk in goal-oriented terms while the traditional definition thinks of risk in event-oriented terms. These two definitions can and do co-exist. They're two different ways of talking about the same phenomena. ISO provides a conceptual definition of risk while the traditional formulation operationalizes this general definition: it explains how to quantify risk. It argues that the amount or level of risk can be calculated by combining probability and severity.
Risk analysis	Risk analysis is a process that is used to understand the nature, sources, and causes of the risks that you have identified and to estimate the level of risk. It is also used to study impacts and consequences and to examine the controls that currently exist. How detailed your risk analysis ought to be will depend upon the risk, the purpose of the analysis, the information you have, and the resources available.

Risk assessment	Risk assessment is a process that is made up of three separate processes: risk identification, risk analysis, and risk evaluation. Risk identification is a process that is used to find, recognize, and describe the risks that could affect the achievement of objectives. Risk analysis is a process that is used to understand the nature, sources, and causes of the risks that you have identified and to estimate the level of risk. It is also used to study impacts and consequences and to examine the controls that exist. Risk evaluation is a process that is used to compare risk analysis results with risk criteria in order to determine whether or not a specified level of risk is acceptable or tolerable.
Risk attitude	An organisation's risk attitude defines its general approach to risk. An organisation's risk attitude (and its risk criteria) influence how risks are assessed and addressed. An organisation's attitude towards risk affects whether or not risks are taken, tolerated, retained, shared, reduced, or avoided, and whether or not treatments are implemented or postponed.
Risk criteria	Risk criteria are terms of reference and are used to evaluate the significance or importance of your organisation's risks. They are used to determine whether a specified level of risk is acceptable or tolerable. Risk criteria should reflect your organisation's values, policies, and objectives, should be based on its external and internal context, should consider the views of stakeholders, and should be derived from standards, laws, policies, and other requirements.
Risk evaluation	Risk evaluation is a process that is used to compare risk analysis results with risk criteria in order to determine whether or not a specified level of risk is acceptable or tolerable.
Risk identification	Risk identification is a process that involves finding, recognizing, and describing the risks that could influence the achievement of objectives. It is used to identify possible sources of risk in addition to the events and circumstances that could influence the achievement of objectives. It also includes the identification of possible causes and potential consequences. You can use historical data, theoretical analysis, informed opinions, expert advice, and stakeholder input to identify your organisation's risks.
Risk management	Risk management refers to a coordinated set of activities and methods that is used to direct an organisation and to control the many risks that can affect its ability to achieve objectives. The term risk management also refers to the programme that is used to manage risk. This programme includes risk management principles, a risk management framework, and a risk management process. Risk & Opportunity Management in a project context: **Risk Management:** Risk management can be described as the process of proactively working with stakeholders to minimise the risks and maximise the opportunity associated with project decisions. **Opportunity Management:** Opportunity management is the process that converts the chance to decisiveness and is increasingly becoming embedded in the culture of organisations as they mature and broaden their understanding of the value that managing uncertainty can bring. For positive risk or opportunity management to be effective in creating or protecting value it must be an integral part of the management processes, be embedded in the culture and practices of the organisation, be tailored to the business process of the organisation, and comply with the risk management principles outlined in ISO 31000. Where risk management seeks to understand what might go badly in a project, opportunity management looks for what might go better.

Risk management framework	According to ISO 31000, a risk management framework is a set of components that support and sustain risk management throughout an organisation. There are two types of components: foundations and arrangements. Foundations include your risk management policy, objectives, mandate, and commitment. And arrangements include the plans, relationships, accountabilities, resources, processes, and activities you use to manage your organisation's risk.
Risk management plan	An organisation's risk management plan describes how it intends to manage risk. It describes the management components, the approach, and the resources that are used to manage risk. Typical management components include procedures, practices, responsibilities, and activities (including their sequence and timing). Risk management plans can be applied to products, processes, and projects, or to an entire organisation or to any part of it.
Risk management policy	A policy statement defines a general commitment, direction, or intention. A risk management policy statement expresses an organisation's commitment to risk management and clarifies its general direction or intention.
Risk management process	According to ISO 31000, a risk management process systematically applies management policies, procedures, and practices to a set of activities intended to establish the context, communicate, and consult with stakeholders, and identify, analyse, evaluate, treat, monitor, record, report, and review risk.
Risk owner	A risk owner is a person or entity that has been given the authority to manage a particular risk and is accountable for doing so.
Risk profile	A risk profile is a written description of a set of risks. A risk profile can include the risks that the entire organisation must manage or only those that a particular function or part of the organisation must address.
Risk source	A risk source has the intrinsic potential to give rise to risk. A risk source is where a risk originates. It's where it comes from. Potential sources of risk include at least the following: commercial relationships and obligations, legal expectations and liabilities, economic shifts and circumstances, technological innovations and upheavals, political changes and trends, natural events and forces, human frailties and tendencies, and management shortcomings and excesses. All of these things could generate a risk that must be managed.
Risk treatment	Risk treatment is a risk modification process. It involves selecting and implementing one or more treatment options. Once a treatment has been implemented, it becomes a control, or it modifies existing controls. You have many treatment options. You can avoid the risk, you can reduce the risk, you can remove the source of the risk, you can modify the consequences, you can change the probabilities, you can share the risk with others, you can simply retain the risk, or you can even increase the risk in order to pursue an opportunity.
Stakeholder	A stakeholder is a person or an organisation that can affect or be affected by a decision or an activity. Stakeholders also include those who have the perception that a decision or an activity can affect them. ISO 31000 2018 distinguishes between external and internal stakeholders.
Strategic Risk	Strategic risks are risks that could affect the achievement of the organisations vision and strategic objectives.
Operational Risk	Operational risks are those which could impact on the organisation's effectiveness and efficiency.

Document Approval

Document Development Officer:	Document Owner:
Manager Governance & Risk (MGR)	Executive Director Corporate & Commercial Services (EDCCS)

Document Control

File Number - Document Type:	CM.STD.7 – Policy
Document Reference Number:	NP21133965
Status of Document:	**Council decision:** Adopted and reviewed.
Quality Assurance:	Executive Management Team, Council Committee, and Council.
Distribution:	Public Document

Document Revision History

Version	Author	Version Description	Date Completed
1.0	RMO	Author: Risk Management Officer (RMO) Adopted by Council on 17 April 2012. Resolution 1.1(4).	17/04/2012
2.0	MGR	Adopted by Council on 28 June 2016, Resolution AR021. Document Reference: NP1223761.	05/07/2016
2.1	MGR	Revised OCM 23/05/2017 Resolution CCCS028. Document Reference: NP1767024	20/06/2017
2.2	MGR	Fully revised and prepared for Audit & Risk Committee and Council review, to reflect changes to standard from (AS/NZS ISO 31000:2009 to AS/ISO 31000:2018).	27/07/2021
3.0	MGR	Adopted by Council on 24 August 2021 Resolution AR098.	07/09/2021
3.1	MGR	Reviewed with delegations in 2022 and 2023. OCM 28/03/2023 Resolution AR131.	20/07/2023