

Risk management policy

Department:	Risk and Procurement
Document ID:	500614
Approved by:	Council – 28 September 2022 [Resolution 22.7.8]
Effective date:	28 September 2022
Next review:	28 September 2023

Purpose

Risk management is an integral aspect of Central Otago District Council operations.

Effective risk management ensures an integrated, structured and coordinated approach to operational risk management throughout all business functions and activities across the organisation. Risk cannot be eliminated entirely; however, it must be clearly understood, ensuring that any risks taken are appropriate for both the business activity and the business level.

This policy aims to support Council's objectives, providing assurance to both Council and the Audit and Risk Committee that risks are being managed appropriately and in line with objectives and the Council's risk appetite.

This policy is in line with the standards of best practice established by the AS/NZS *ISO31000:2018 Risk Management – Principles and Guidelines*. This shall be achieved through the continual implementation of risk management throughout processes within the organisation and creating a strong organisational risk aware culture.

Principles and objectives

Central Otago District Council's risk management processes are applied in accordance with the following objectives.

- Embed a consistent risk management process with the implementation of a common approach to the identification, assessment, treating and monitoring of risks;
- Provide protection and continuity of core business activities;
- Promote a risk aware culture whereby all employees assume responsibility and proactively manage risk through sound decision making in their day to day activities;
- Define and establish clear responsibilities and structures to ensure risk management practices are incorporated into strategic, operational and project planning and review processes;

- Establish a consistent, clear framework to provide assurance that material risks are identified, regularly reviewed, monitored and managed to an acceptable level, in an open and transparent manner.

Scope

This policy applies to all business, service or activity conducted by Council and all employees of Council.

For the avoidance of any doubt, any reference to employees or staff in this policy include:

- the organisation's employees
- volunteers
- persons seconded to council
- contractors.

Elected members are excluded from this definition.

Specific risk management policies, procedures and/or guidelines relating to specialised areas remain consistent with the broad directions in this policy.

Definitions

Word or phrase	Definition
Risk	The effect of uncertainty on objectives (adopted from the AS/NZS ISO 31000-2018 Risk Management Standard). Risk may be something unexpectedly occurring which impacts negatively upon council's strategic objectives. Risk is assessed in terms of likelihood and consequence.
Risk Assessment	The overall process of risk identification, risk analysis and risk evaluation.
Risk Management	An enabling function which adds value to the organisation, increasing the probability of success in achieving strategic objectives. Risk management aims to decrease the potential for legal liability and managing uncertainty; creating an organisation wide environment where the unexpected is minimal and, should it occur, the consequences may be managed effectively.

Word or phrase	Definition
Risk Management Framework	The set of components which provide foundations for designing, implementing, monitoring, reviewing and continually improving risk management within the organisation. Components include the Risk Management Policy, Process, Risk Registers.
Risk Management Process	The systematic and consistent application of policies, processes and practices of establishing the context, identifying, analysing, evaluating, communicating, treating, monitoring and reviewing risk.
Risk Register	A documented record of risks identified. This includes a description of risk, controls, risk levels and treatment plans.
Risk Appetite	The level of risk that council is willing to accept in pursuit of its strategic objectives.
Risk Tolerance	A measure of the level of risk an organisation is willing to accept, used as a key criterion when making risk-based decisions.
Risk Owner	The position with authority and accountability for managing a specific risk and any associated risk controls.

Roles and responsibilities

All staff

Risk Management is the responsibility of all Central Otago District Council staff. The process of identifying and managing risk should underpin all council functions to ensure transparency, authority and accountability. To remain effective, both the Risk Management Policy and Framework must be supported by an organisation-wide risk aware culture which will better enable council to achieve strategic goals.

Specific duties by role

To support the Risk Management Framework and ensure an appropriate degree of oversight, transparency and accountability in risk management practices around the organisation, the roles and responsibilities have been outlined in *Appendix One: Risk Management Roles and Responsibilities*.

Policy

Central Otago District Council shall maintain an effective and relevant Risk Management Framework, ensuring a structured, consistent and systematic approach to risk management across the organisation. Risk management documents shall remain relevant to the organisational culture, business objectives and organisational strategies, remaining applicable to all areas and in keeping with Council's risk appetite.

Core Principles

Central Otago District Council establish, implement, maintain and monitor effective risk management processes aligned with the principles and processes described within AS/NZS ISO31000:2018 *Risk Management – Principles and Guidelines*. The following core principles are the foundation for Council Risk Management Processes.

- Facilitation of a risk-aware culture which is integrated into all critical planning and decision-making activities;
- Systematic, structured, transparent, informed and inclusive processes with the engagement of all relevant stakeholders, both internal and external where appropriate, contributing to risk discussions;
- Identifying, assessing, treating and monitoring risks throughout the organisation;
- Recognising and integrating strategic, operational, human and cultural factors into processes;
- Maintaining dynamic and customisable yet resilient risk management processes which are responsive, adapting to a changing environment and Councils risk appetite in a timely manner;
- Reduce the likelihood of negative impacts on Council's strategic directives/objectives by obtaining the best possible information to base decisions from;
- Recognise, respect and support human and cultural factors which may influence risk management decisions.
- The Central Otago District Council Risk Management Framework includes but is not limited to the following:
 - Central Otago District Council Risk Management Policy – provides guidance and a foundation for the management of risk.

- Central Otago District Council Risk Management Process – provides guidance on identification of potential threats to an organisation and defines the strategy for eliminating, mitigating and/or minimising the impact of these risks, as well as processes to effectively monitor and evaluate this strategy.
- Central Otago District Council Strategic Risk Register – register of the organisations strategic and operational risk, with the inclusion of risk ratings and management/treatment plans.
- Central Otago District Council Group Risk Register – risk Register for each business area with the inclusion of risk ratings and management/treatment plans.
- Audit and Risk Committee – the overarching governance body assisting and advising Council in meeting the responsibility and ownership of governance, risk management and internal controls to achieve strategic objectives.
- Relevant information, training and educational activities for the ongoing improvement of risk management processes.
- Informed decisions are to be made based on a comprehensive understanding of the risks involved; It is acknowledged that some risks must be accepted in the achievement of strategic objectives.

Risk Reporting

Reporting of risk is an integral aspect of effective risk management, aiming to support the understanding of risk at all levels - to improve decision making, day to day operations and the achievement of objectives. Risk reporting is a fluid and constantly evolving process.

Risk reporting should focus on the change to the risk profile, outlining any emerging or potential risks which may require escalation.

Risk reports are prepared annually for the Executive Team and bi-annually for the Audit and Risk Committee. Risk management includes continual communications with both internal and external stakeholders.

Risk reporting details the following.

- Risks which stand outside accepted tolerance levels
- Escalating risks
- Emerging risks
- Significant project risks.

Comprehensive reporting on significant risks contributes to effective governance.

Relevant legislation

AS/NZS ISO 31000:2018 Risk Management – Principles and Guidelines

Reporting and Monitoring

The policy is reviewed every three years or as required.

Related documents

- Staff Interest Policy
- Fraud, Bribery and Corruption Policy
- Fraud, Bribery and Corruption Process
- Protected Disclosure (Whistle blower) Policy
- Delegations Policy
- Register of Interest

Document Management Control:

Prepared by: Business Risk and Procurement Manager

File Location Reference: 500614

Date Issued: 26 August 2020

Attachments

Appendix One:	Risk Management Roles and Responsibilities
Appendix Two:	Risk Likelihood Table
Appendix Three:	Risk Consequence Table
Appendix Four:	Risk Matrix

Appendix One

Risk Management Roles and Responsibilities

Position	Roles and Responsibilities
Audit and Risk Committee	<ul style="list-style-type: none"> • The Audit and Risk Committee provides governance and oversight in the areas of audit and risk to ensure appropriate systems and best practices are delivered throughout the organisation and its activities. • Ensure that strategic planning and business operations are achieved within an effective Risk Management Framework. • Review and recommend approval of risk management frameworks, risk-related policies, the Risk-Register and review risk treatment options for critical risks. • Supervise Corporate Risk Registers • Monitor and review the risk management practices, systems and processes adopted by Council to ensure these remain relevant and appropriate. • Monitor Council's risk appetite and exposure and recommend to Council any pre-emptive or corrective actions in respect of risk management frameworks, the Risk Register and risk-related policies. • Approve and monitor the internal auditor's annual workplan, ensuring an adequate response to corrective actions are assumed and implemented.
Council	<ul style="list-style-type: none"> • Nominate members for the Audit and Risk Committee. • Confirm appropriate risk governance and management frameworks are in place, ensuring risks are appropriately managed, aiding in the achievement of Council's strategic objectives. • Receive and evaluate reports from the Audit and Risk Committee.
Chief Executive Officer	<ul style="list-style-type: none"> • Lead and promote a risk-aware culture across the organisation. • Ensure overall accountability, authority and resources for managing risks within management and operational areas. • Champion a strong risk management culture across the organisation. • Report critical risks to Council with treatment options.
Executive Manager – Corporate Services	<ul style="list-style-type: none"> • Oversee the development and implementation of the Risk Management Policy and Risk Management Framework. • Ensure that the Risk Framework and Corporate Risk Register are regularly reviewed and maintained and inform the development and effectiveness of risk controls and management plans implemented.

Position	Roles and Responsibilities
	<ul style="list-style-type: none"> • Ensure appropriate reporting to the Audit and Risk Subcommittee and Council. • Receive disclosures from all members of staff relating to risk concerns or issues. • Review tracking of risks against the Risk Appetite tolerance limits.
Executive Team	<ul style="list-style-type: none"> • Champion a strong risk management culture across all of Council. • Maintain situational awareness of council-wide risk exposure, priorities and risk management activities. • Ensure the effective implementation of the organisation-wide Risk Management Framework and promote a risk-aware culture across the organisation. • Develop and maintain an effective Risk Management Policy. • Facilitate the identification, management and monitoring of the organisations Strategic and Operational Risks. • Undertake (at a minimum) a six-monthly review of the Corporate Risk Register, and the appropriateness of all Strategic Risk ratings, priorities, controls and management plans. • Monitor relevant Group Risk Register/s and ensure the appropriateness of all associated risk ratings, priorities, controls and management plans. • To facilitate the management of organisation-wide risks and risk management training.
Business Risk and Procurement Manager	<ul style="list-style-type: none"> • Responsible for the maintenance of the Risk Management Framework. • Support the development and provision of risk training and awareness-raising activities across the organisation. • Facilitate (at a minimum) a six-monthly review of the Corporate Risk Register, and inform associated risk ratings, priorities, controls and management plans. • Support the development of relevant business (BAU, project, contract) risk registers and appropriate risk management plans, activities and priorities, including providing specialist advice in relation to new or existing risks, appropriate management strategies and the escalation of risks. • Provide reports to, the Executive Team and the Audit and Risk Committee on Council's Strategic and Operational Risk exposure, to ensure effective oversight and assurance of all business risk management activities. • Alongside the Audit and Risk Committee, develop and manage the delivery of Council's annual internal audit plan and activities. • Support the activities of Council's Audit and Risk Committee.

Position	Roles and Responsibilities
	<ul style="list-style-type: none"> • In conjunction with the Executive Team, develop and review the Risk Management Policy and Risk Management Framework. • Receive disclosures from all members of staff relating to risk concerns or issues.
Managers	<ul style="list-style-type: none"> • Champion a risk-aware culture across the organisation and their group and drive implementation of the Risk Management Framework. • Develop and maintain relevant business (BAU, project, contract) risk registers and appropriate risk management plans, activities and priorities. • Implement risk management practices within relevant business areas. This includes ensuring that all operational risks are effectively identified, managed, reviewed and updated regularly. • Report all risks with a residual risk rating of high and critical to the Group Manager and/or Business Risk and Procurement Manager for review. • Prioritise resources, time and budget to those risks rated high and very high; and implement appropriate risk controls or business improvement activities. • Facilitate the identification, management and monitoring of Council's Strategic and Operational Risks, ensuring Risk Management is incorporated into the planning and delivery of the Council's core strategic and business activities. • Undertake (at a minimum) a six-monthly review of the Corporate Risk Register, and the appropriateness of all Operational Risk ratings, priorities, controls and management plans. • Develop and monitor respective Group Risk Register/s and ensure the appropriateness of all associated risk ratings, priorities, controls and management plans. • Alongside the Business Risk and Procurement Manager, facilitate the delivery of the annual internal audit plan and activities, and appropriate corrective or business improvement activities within their group.
All Staff	<ul style="list-style-type: none"> • To maintain awareness of risks, risk management and processes associated with risk management. • Ensure compliance with the Risk Management Policy. • Apply risk management practices in all day-to-day business activities. This involves systematically identifying, assessing and treating risks in accordance with the Risk Management Framework. • Ensure that risk management reporting is appropriately undertaken and advise their Manager, or the Business Risk and Procurement Manager of any risks residually rated as high or critical or that they believe require attention.

Position	Roles and Responsibilities
	<ul style="list-style-type: none"> Maintain an awareness of current and potential/emerging risks that relate to their area of responsibility. Support the implementation of risk mitigation.

Appendix two

Risk Likelihood Table

Score	Rating	Probability	Frequency	Likelihood Criteria
5	Almost Certain	>90%	Frequency of more than once a year	<ul style="list-style-type: none"> Is expected to occur Definite probability
4	Likely	60% - 90%	Frequency of occurring once a year	<ul style="list-style-type: none"> Will probably occur
3	Moderate	20% - 60%	Frequency of occurring once every 5 years	<ul style="list-style-type: none"> Could occur
2	Unlikely	5 – 20%	Frequency of occurring once in 5 -10 years	<ul style="list-style-type: none"> Not generally expected to occur The event hasn't occurred, but could
1	Rare	<5%	Once every 20 – 50 years.	<ul style="list-style-type: none"> Exceptional circumstances Improbable Small chance of the event occurring Caused by events and/or conditions previously unseen

Appendix three

Risk Consequence Table

Risk consequence category	Negligible	Minor	Moderate	Major	Extreme
	1	2	3	4	5
People and Health and Safety	No injury/harm. A possible near miss.	Minor injury or harm. Medical treatment required	Moderate injury or harm. One or more persons require medical treatment.	Serious injury or harm.	One or more fatalities or permanent disability or injury.
Compliance and legal/statutory and regulatory	Negligible compliance breach. Able to be remedied without penalty or notification.	Minor compliance breaches resulting in corrective actions.	Moderate statutory or regulatory breaches resulting in formal investigation by regulatory body, Council liability and fines may be provided.	Major statutory or regulatory breaches and litigation. External investigation, litigation, fines and implications for Executive Team.	Very serious statutory or regulatory breaches and litigation Serious court enforcement, prosecution or judicial review.
Environmental	Brief, non-hazardous and short-term impact on localised natural environment or ecosystem. Minor short-term reversible damage to landscapes	Minor damage including temporary pollution or contamination of localised natural environment or ecosystem. Minor reversible damage to landscapes. Temporary reduction of one or more of species.	Widespread damage to local natural environment and ecosystems taking several years to recover and extensive restoration work. Localised reversible damage to landscapes. Moderate reduction of one or more species.	Long-term and significant damage to natural environment and ecosystems taking >5 years to recover and significant restorative work. Localised irreversible damage to landscapes. Significant reduction in one or more species.	Irreversible and extensive damage to significant natural environments and ecosystems. Widespread irreversible damage to landscapes. Permanent loss of one or more species.
Reputation and stakeholder relationship	External Reputation not affected. No effort or expense required to recover.	Adverse attention from community groups and district media – no more than 1 day.	Regional and district media attention short term (1-3 days). Partial loss of stakeholder confidence.	Nationwide media attention, more than 3 days. Significant reduction in stakeholder confidence.	Prolonged adverse national media attention. Significant long-term reduction in stakeholder confidence.

Risk consequence category	Negligible	Minor	Moderate	Major	Extreme
	1	2	3	4	5
			Negative association with CODC brand. little effort or expense required to recover.	Negative association with CODC brand. Requires effort or expense to recover and mitigate.	Potential statutory management intervention. Significant damage to CODC brand requiring urgent effort and expense to recover. Involves unplanned council time to address.
Financial	Less than 10% loss of revenue, increase in expense or liability.	Between 10% and 19% loss of revenue, increase in expense or liability.	Between 20% and 29% loss of revenue, increase in expense or liability.	Between 30% and 49% loss of revenue, increase in expense or liability.	Greater than 50% loss of revenue, increase in expense or liability.
Performance and Capability	A disruption to any service or activity that causes an inconvenience for less than 4 hours. (half a workday) Negligible performance impact.	Minor impact on the quality or delivery of services offered. Disruption to any service or activity lasting less than one day	Some impact on the quality or delivery of services offered. 1 critical service or numerous non-critical service activities which are undeliverable for a minimum of one week.	Considerable impact on the quality or delivery of services offered. Impedes the achievement of objectives. One or a number of critical activities are undeliverable for a period between 2-4 weeks.	Major impact on the quality or delivery of services or operation. Sustained inability to deliver core services. One or a number of critical services or activities are unavailable for a period of more than one month.
Assets and Infrastructure	Impairment of a non-critical asset which causes an inconvenience for less than 4 hours. Minor damage to an asset	Impairment of a non-critical asset which interrupts service delivery for less than 1 day. Damage to an asset	Damage to one or more critical assets which interrupts service delivery for at least 1 week. Damage to multiple assets	Extensive damage to one or more critical assets which interrupts service delivery for a month. Loss of an asset	Damage to multiple critical assets which interrupts service delivery for more than 1 month. Loss of multiple assets
IS Systems and Data	Non-critical systems or data	Loss of access to non-critical systems or data	Loss of access to critical systems	Loss of access to critical systems and data for	Loss of access to critical systems

Risk consequence category	Negligible	Minor	Moderate	Major	Extreme
	1	2	3	4	5
	interrupted for less than 4 hours.	for less than 1 day.	and/or data for at least 1 week.	between 2 to 4 weeks.	and data for more than 1 month.

Appendix four

Risk Matrix

Likelihood rating		Consequence rating				
		Negligible	Minor	Moderate	Major	Extreme
		1	2	3	4	5
Almost certain	5	Medium	Medium	High	Critical	Critical
Likely	4	Low	Medium	High	High	Critical
Moderate	3	Low	Medium	Medium	High	Critical
Unlikely	2	Low	Low	Medium	High	High
Rare	1	Low	Low	Low	Medium	High

Likelihood rating		Consequence rating				
		Negligible	Minor	Moderate	Major	Extreme
		1	2	3	4	5
Almost certain	5	Medium (5)	High (10)	High (15)	Critical (20)	Critical (25)
Likely	4	Medium (4)	Medium (8)	High (12)	Critical (16)	Critical (20)
Moderate	3	Low (3)	Medium (6)	Medium (9)	High (12)	High (15)

Unlikely	2	Low (2)	Medium (4)	Medium (6)	Medium (8)	High (10)
Rare	1	Low (1)	Low (2)	Low (3)	Medium (4)	Medium (5)

Low	1 – 3
Medium	4 - 9
High	10 - 15
Critical	16 - 25