Invercargill
CITY COUNCIL

Risk Management Policy

Purpose

This Policy sets out Invercargill City Council's (Council) mandatory requirements for effective risk management. It defines roles and responsibilities, establishes the principles and processes aligned with ISO 31000:2018 Risk Management - Guidelines, and describes how risks are identified, assessed, treated, communicated, monitored and reviewed to support the achievement of organisational objectives, meet legal and regulatory obligations, maintain public confidence, and improve performance and service delivery.

Scope

This Policy applies to Council employees, Elected and Appointed Members, contractors (including subcontractors), consultants, and volunteers. This Policy does not apply to Council Controlled Organisations (CCOs) but it is expected that CCOs will have a risk management policy and framework consistent with Council's.

Overview

Council is committed to the informed management of risks in order to effectively and efficiently reduce, monitor, and control the negative effect risk can have on the achievement of organisational objectives.

This Policy sets out mandatory requirements for risk management. Council is committed to keeping its risk management approach relevant and applicable to all areas of operation by using the ISO 31000:2018 Risk Management Standard as its basis.

For risk management to be effective it must be an integral part of the development of organisational strategy and day-to-day operations. This Policy outlines Council's three lines model that provides a principles and risk based approach to ensuring effective governance, risk management, and internal control. This model delineates responsibilities across three distinct lines of assurance, enhancing accountability and transparency in managing risks, and achieving organisational objectives.

Council also develops and regularly reviews its Risk Management Framework. The Risk Management Framework records Council's current risk appetite and risk tolerance, which are developed in line with the principles of this Policy.

Definitions

Consequence: the outcome of an event affecting objectives.

Control: a measure that modifies the risk, for example processes or physical constraints that change the likelihood of an event occurring or impact the consequences.

Inherent risk: the level of risk prior to the implementation of controls.

Likelihood: the chance of something happening.

Residual risk: the level of risk remaining after controls and treatments are considered.

Risk: the effect of uncertainty on objectives.

Risk appetite: the amount and type of risk Council is willing to accept in pursuit of its objectives.

Risk assessment: the overall process of risk identification, risk analysis, and risk evaluation.

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

Risk Management Framework: the document which records the set of components which provide foundations for designing, implementing, monitoring, reviewing, and continually improving risk management within the organisation.

Risk owner: the person with the accountability and authority to manage the risk and the treatment plan.

Risk Management Process: the systematic and consistent application of policies, processes, and practices of establishing the context, identifying, analysing, evaluating, communication, 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 tolerance: the amount of risk Council is ready to bear temporarily, taking into account cost, timing, and constraints.

Governance, Roles, and Responsibilities (Three Lines Model)

Council uses the Institute of Internal Auditors' Three Lines Model, which helps identify structures and processes to facilitate strong governance and risk management. Using the Three Lines Model, Council has identified the following roles and responsibilities:

Council (Governing body)

- Adopts the Risk Management Policy.
- Determines Council's risk appetite (to be recorded in the Risk Management Framework) and exercises oversight of risk management.
- Delegates risk governance oversight to the Risk and Assurance Committee.
- Holds the Chief Executive to account for risk management effectiveness.

Risk and Assurance Committee (Governing body)

- Provides independent oversight of risk management systems, processes and practices.
- Reviews whether management has in place a current and comprehensive Risk Management Framework and associated procedures for effective identification and management of Council's financial and business risks, including fraud.
- Reviews whether a sound and effective approach has been followed in developing risk management plans for major projects and significant risks.
- Receives quarterly reports on High and Extreme risks and material changes to Council's risk profile.

Chief Executive (Management)

- Maintains primary accountability to Council for risk management.
- Approves the Internal Audit/Assurance Programme.
- Escalates material changes in risk profile to Council/Risk and Assurance Committee.
- Ensures adequate resources and systems are in place.

Executive Leadership Team (Management)

- Reviews and recommends the Policy and Risk Management Framework risk appetite for adoption.
- Maintains situational awareness of organisational risk context and interconnections.
- Directs deep-dive reviews of key strategic, operational, and programme/project risks.
- Receives risk reports and prioritises treatment activity.

Group Managers (Management)

- Own and oversee risks within their groups; ensure timely treatment and reporting.
- Escalate High and Extreme residual risks to Executive Leadership Team.
- Monitor overdue treatments and ensure control effectiveness reviews occur.

Manager – Risk and Continuous Improvement (Second Line)

- Develops and maintains the Risk Management Policy and Framework.
- Coordinates periodic reviews of strategic and operational Risk Registers and facilitates risk workshops.
- Provides systems, guidance, challenge and monitoring; reports quarterly to Executive Leadership Team and Risk and Assurance Committee.
- Supports identification of risk interconnections and integrated treatment planning.

All staff, contractors, and volunteers (First Line)

- Identify, record, analyse, and evaluate risks in their activities in line with the Risk Management Policy and Framework.
- Implement approved treatment plans and monitor effectiveness.
- Escalate risks per the reporting thresholds.

Internal Audit (Third Line)

- Provides independent and objective assurance and advice on governance, risk management and internal controls.
- Reports material findings to the Chief Executive and Risk and Assurance Committee; safeguards independence.

Risk Management Principles

Council's approach to risk management is aligned to ISO 31000:2018 and is:

- Integrated;
- Structured and comprehensive;
- Customised;
- Inclusive;
- Dynamic;
- Based on the best available information;
- Cognisant of human and cultural factors; and
- Committed to continual improvement.

Risk Management Process

Risk management at Council follows the ISO 31000:2018 process:

- Communicate and consult;
- Establish scope, context, and criteria;
- Identify risks;
- Analyse;
- Evaluate;
- Treat;
- Monitor, review and report.

Risk Types and Categories

Council recognises the following risk types:

- Strategic,
- Operational,
- Programme/Project.

Council uses the following risk categories for consequence scaling and appetite:

- Financial sustainability,
- People and knowledge,
- Service delivery, critical services,
- Legal and regulatory compliance, privacy
- Health, safety and wellbeing,
- Information management, cyber,
- Environment and climate resilience,
- Projects and property,
- Reputation, community trust,
- Achievement of strategic objectives (opportunities).

Risk Assessment

Risk assessment comprises the following steps:

- **Identify** – All staff identify and record risks in the Risk Register.
- **Analysis** – Determine likelihood and consequence without controls. Council rates likelihood on a scale from rare to almost certain, and consequence from very minor to catastrophic, as detailed in the Risk Management Framework. Determine inherent risk using the matrix in the Risk Management Framework, assess control effectiveness, and determine residual risk.
- **Evaluation** – Compare residual risk to appetite/tolerance.

Risk Treatment

The following measures are recognised as potential options for risk treatment:

- **Avoid** – do not start/continue the activity, or remove the risk source.
- **Reduce** – implement additional controls to change likelihood and/or consequence.
- **Transfer/Share** – use tools such as contracts or insurance.
- **Accept/Retain** – informed decision where within appetite, with monitoring.
- **Increase** – in appropriate cases, an informed decision to pursue opportunities.

Treatment plans will specify accountable owner, milestones, resources, target risk level and review dates.

Risk Appetite

Risk appetite is the amount and type of risk Council is willing to accept in pursuit of its objectives, strategic priorities and community outcomes.

Council sets its overall risk appetite through the Risk Management Framework and exercises oversight of how it is applied. The detailed articulation of risk appetite, including category-specific appetite statements, tolerance boundaries, and guidance on acceptable and unacceptable risk-taking, is also documented in the Risk Management Framework.

The Risk Management Framework:

- Describes how risk appetite and tolerance are applied in practice;

- Supports consistent risk evaluation, escalation and acceptance decisions; and
- Enables risk appetite settings to be reviewed dynamically and refined in response to changes in Council's operating environment, strategic direction, and risk profile.

When assessing, evaluating, and treating risks, all staff and decision-makers must apply the risk appetite and tolerance settings as set out in this Policy and the Risk Management Framework.

Recording, reporting, and review

Recording

All risks are recorded in the Risk Register. Programme/project and Health, Safety and Wellbeing risks may be managed in specialist registers and systems appropriate to their nature. Health, Safety and Wellbeing risks are governed by the Health, Safety and Wellbeing Policy and associated procedures, and must be managed in a manner that is consistent with this Risk Management Policy and the Risk Management Framework.

Reporting and review

Reporting, review, and ownership requirements are dependent on the level of residual risk, as follows:

Residual level	Minimum owner	Reporting requirements	Review requirements
Extreme	Chief Executive or delegate	Quarterly to Executive Leadership Team and Risk and Assurance Committee, immediate escalation on material change	Weekly
High	Group Manager or delegate	Quarterly to Executive Leadership Team and Risk and Assurance Committee	Monthly
Medium	Group Manager or Tier 3 Manager	Six-monthly to Executive Leadership Team	Monthly
Low	Tier 3 / Tier 4 Manager	Six-monthly to Executive Leadership Team (summary)	Every two months
Insignificant	Tier 3 / Tier 4 Manager	As required	Annually

All High and Extreme risks are reported to the Risk and Assurance Committee at least quarterly.

Assurance

The Internal Audit function (or outsourced provider) develops a risk-based Internal Audit/Assurance Programme. The Chief Executive approves this annual internal audit programme of work on an annual basis. Material findings and status of actions are reported to the Risk and Assurance Committee quarterly.

Relevant Legislation and Related Documents

- Local Government Act 2002
- Protected Disclosures (Protection of Whistleblowers) Act 2022
- Serious Fraud Office Act 1990
- Protected Disclosures and Internal Complaints Policy
- Financial Risk Management Policy
- Health, Safety and Wellbeing Policy
- Elected and Appointed Members Expenditure and Allowances Policy
- Conflicts of Interest Policy
- Code of Conduct for employees

Document Control

Revision History:	
Effective Date:	23 June 2026
Review Period:	This Policy will be reviewed every three (3) years, unless earlier review is required due to legislative changes, or is warranted by another reason requested by Council.
New Review Date:	June 2029
Associated Documents / References:	Risk Management Framework
Supersedes:	Risk Management Framework – Policy and Process
Reference Number:	A6330620
Policy Owner:	Manager – Risk and Continuous Improvement
Policy Training:	All staff