CENTRAL OTAGO DISTRICT COUNCIL

1 Dunorling Street
PO Box 122, Alexandra 9340
New Zealand

03 440 0056

Info@codc.govt.nz
www.codc.govt.nz

Risk Management Policy

Department:	**Business Support**
Document ID:	1385002
Approved by:	Council – 29 January 2025
Effective date:	January 2025
Next review:	October 2027

Contents

Purpose **3**
Scope and Audience **3**
Background **3**
Policy **3**
Risk Management Principles 3
Risk Management Practices 4
Risk Management Approach 4
Risk Categorisation 5
Risk Management Framework 6
Risk Management Framework RACI 6
Risk Management Process 8
Risk Identification 9
Risk Assessment 9
Inherent Risk Assessment of Operational and Key Risks 9
Risk Treatment 10
Residual Risk Assessment of Operational and Key Risks 10
Current Risk Assessment of Project Risks 10
Target Risk Ratings for Project Risks 10
Risk Appetite 10
Risk Acceptance 10
Operational Risk Management 11
Project Risk Management 11
Key Risk Management 12
Operational Risk Event Management 13
Risk Reporting and Committee Review 14
Ongoing Monitoring and Training 14
Glossary **14**
Related Documents **15**
Appendix 1 – Impact Criteria Key and Operational Risks **16**
Appendix 2 - Likelihood Criteria Key and Operational Risks **17**
Appendix 3 – Impact Criteria (Project Risks) **18**
Appendix 4 - Likelihood Criteria (Project Risks) **19**
Appendix 5 – Risk Matrix **20**

Purpose

This policy contains details of the risk management approach to be followed by Central Otago District Council (CODC or Council). The policy details the methods used to identify, assess, manage, and report on risk. The policy makes reference to different types of risk and details the differing approach to the management of each.

Scope and Audience

This policy applies to all employees and governing body members of CODC. This includes:

- A Council staff member;
- A consultant who is provided with system access and a CODC email address;
- Elected Members; and
- Appointed Members.

This policy does not apply to external contractors, external consultants, Council Controlled Organisations, or joint ventures. However, these parties should be encouraged to follow risk management best practice and can be provided with this policy if required.

Background

Council recognises that sound risk management is a function that will support better decision-making, increase awareness of potential issues, and strengthen the organisation's capability and maturity. As such, CODC aims to utilise this policy to increase effectiveness, improve the risk maturity of the organisation and foster a culture of risk awareness.
This policy is aligned to the principles of the ISO31000:2018 Risk Management Standard.

Policy

Risk Management Principles

CODC's Risk Management Framework is governed by the following principles:

- Successful risk management contributes to the achievement of objectives, improves decision making, and supports improvement of performance.
- Staff and Elected Members are provided with the training, tools, and support required to manage risk effectively.
- Embracing risk management from the top down enables a strong risk-aware culture.
- Risk management is transparent and involves stakeholders and decision makers at all levels.
- Risk management is a practice that is dynamic, responds to change, and aims to continuously improve.
- Whilst accountability is required, a no-blame culture is integral to the success of an embedded risk management framework.

Risk Management Practices

Embracing the following practices will improve risk awareness and support adherence to this policy:

- Employees must be aware of and own their responsibilities in relation to risk management;
- Executive Leadership and Management Teams must lead a culture of risk awareness;
- Employees must report risks, issues, and losses to a manager, or the Risk & Procurement Manager as soon as is reasonably practicable; and
- Employees should be open and transparent when identifying, managing, and reporting on risk.

Risk Management Approach

CODC's Risk Management Framework comprises four main elements:

1. Operational Risk Management
2. Project Risk Management
3. Key Risk Management
4. Operational Risk Event Management

CODC aims to identify and manage all types of risk faced by the organization and the community. Risks are documented in one of three documents:

1. Key Risk Register
2. Operational Risk Register
3. Project Risk Register

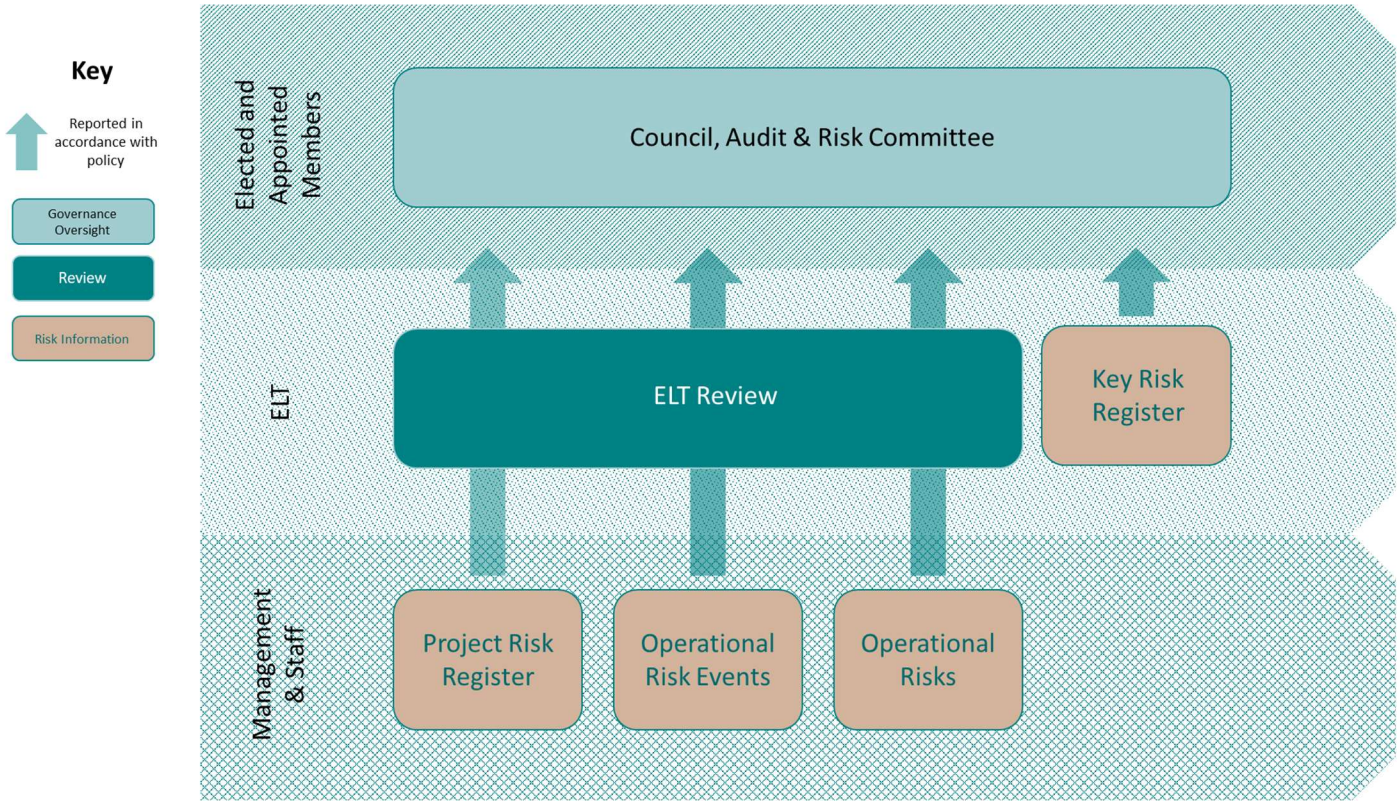
Risk Categorisation

Risks are categorised and documented in the appropriate format, as show in the table below.

Risk Type	Sub-category	Description	Documented within
Financial	Credit	The risk that a counterparty may default of their obligations (a given financial claim is not paid in full) or have their credit rating downgraded.	Key Risk Register
	Liquidity	The risk that an organisation is unable to meet its financial liabilities as they fall due.	
	Market	The risks that arise due to fluctuations in the value of, or income from, the assets of an organisation.	
Operational	People	Risk of loss resulting from inadequate numbers of skilled/trained internal people.	Operational Risk Register
	Process	Risk of loss resulting from inadequate or failed internal processes.	Key Risk Register
	Systems	Risk of loss resulting from inadequate or failed internal systems.	
	External	Risk of loss resulting from an external event.	
Strategic	N/A	Risks that are created or affected by the chosen strategy of an organisation.	Key Risk Register
Project	N/A	Risks associated with the design, implementation, and delivery of a project. Most of these risks should close with the project, but some may be transferred to Business-as-Usual dependent on what is being delivered by the project.	Project Risk Register

Risk Management Framework

The diagram below shows ownership of sources of risk information and how these are connected and reported to the Audit and Risk Committee.



Risk Management Framework RACI

The RACI (Responsible, Accountable, Consulted, Informed) Table below shows how staff and Elected Members are involved in all elements of the framework.

In addition to the details below, referring to specific framework responsibilities, all Elected and Appointed Members have a responsibility to provide oversight and challenge on matters relating to risk management, ensuring that their governance responsibilities are discharged appropriately to support the effective management of risks faced by Council and the community.

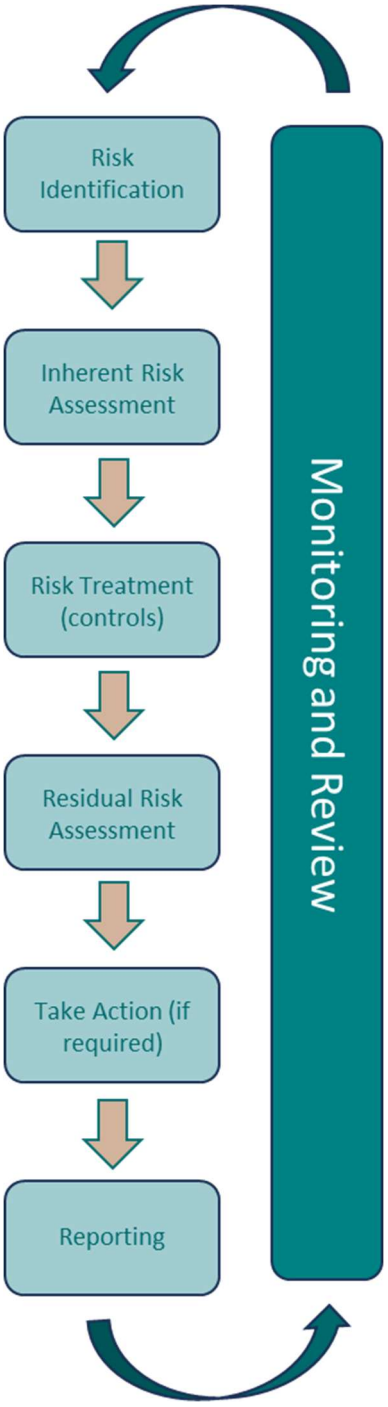
Risk Management Framework RACI Table

RACI Element	RACI Description	Operational Risk Management	Project Risk Management	Key Risk Management	Operational Risk Event Management
Responsible	The person who will be held responsible for the completion of the task	Activity Managers	Project Managers	Executive Leadership Team	All staff members – responsible for identifying and notifying management of events. Management – responsible for planning or taking action required
Accountable	The person who must oversee the completion of the task	Executive Leadership Team	To be defined in the Project Management Framework	Chief Executive	Executive Leadership Team
Consulted	The person (or people) providing advice or guidance on the task or outputs	Risk & Procurement Manager Audit and Risk Committee	Risk & Procurement Manager Audit and Risk Committee	Risk & Procurement Manager Audit and Risk Committee	Risk & Procurement Manager Audit and Risk Committee
Informed	Those who must be informed when the task is completed	Executive Leadership Team Audit and Risk Committee	Executive Leadership Team Audit and Risk Committee	Audit and Risk Committee	Executive Leadership Team Audit and Risk Committee

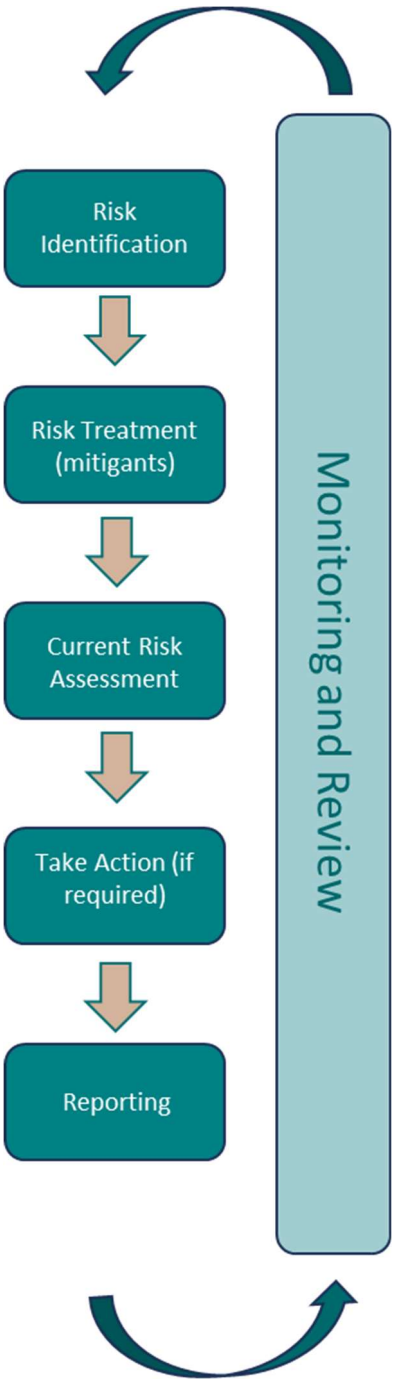
Risk Management Process

The risk management process at CODC is informed by the ISO3100:2018 Risk Management Process. The process differs between management of Operational and Key Risks and Project Risks, as shown by the two diagrams below.

Operational & Key Risk Management



Project Risk Management



Risk Identification

CODC understands that risks can be identified using many different methods and sources of information. Different approaches may be used to identify risks to be documented in each register type. Considerations for each register type are listed below.

Operational Risks Registers (Operational Risks):

- Unit processes, priorities, and objectives
- Legislative requirements
- Discussion with activity managers, team leaders, and team members
- Suggestion from ELT
- Issue Management
- Operational Risk Events (whether isolated or repeated)
- External events
- Audit reports and recommendations
- Changes to legislation
- Change to department activity

Key Risk Register (Strategic, Operational, Financial Risks):

- Discussion with ELT Members
- Suggestion from Elected Members
- Issue Management
- Loss Events (whether isolated or repeated)
- Increased risk exposure noted in Operational Risk Registers
- External events
- Audit reports and recommendations
- Legislative requirements
- Changes to legislation
- Change to activity performed by Council

Project Risk Register (Project Risks):

- Circumstances that could impact delivery of the project on time, within budget, and to specification
- Project activity that could have a negative impact on the wider business
- Stakeholder interest and management
- External factors

Risk Assessment

In order to establish risk exposure, each risk is assessed against Impact and Likelihood criteria on a 1-5 scale. Impact and Likelihood scores are multiplied, resulting in an overall risk score of between 1 and 25. These scores represent a risk exposure of very low, low, medium, high, or very high. The approach for Operational Risk and Key Risk Registers differs to the approach for Project Risk Registers.

Inherent Risk Assessment of Operational and Key Risks

Inherent Impact and Likelihood Assessments are undertaken and documented, providing details of exposure if no controls were in place.
Inherent assessments must not be extreme and should be considered in the context of staff members aiming to ‘do their best’, without controls being formally implemented.
Impact and Likelihood assessment criteria for Operational and Key Risks can be found at Appendix 1 and 2.

Risk Treatment

All risks must have associated controls or mitigants documented. Where controls or mitigants are not currently being undertaken, action is required to implement required activities.

Residual Risk Assessment of Operational and Key Risks

Residual Impact and Likelihood Assessments are undertaken and documented, providing details of exposure following implementation of controls.
In addition to considering the impact and likelihood of a risk occurring, the existing control environment must be taken into account when assessing risks at a residual level. This means that existing controls must be reviewed to ensure detail remains accurate and up to date, the controls are performing as expected, and any additional controls are identified and documented.
Through the process of risk assessment, the need for further action may be identified. This may be as a result of a risk being assessed as out of appetite, or because controls have been found to be missing or ineffective.
Impact and Likelihood assessment criteria for Operational and Key Risks can be found at Appendix 1 and 2.

Current Risk Assessment of Project Risks

Project Risks are not assessed at an Inherent level, but rather an assessment is made of the current exposure, with mitigating actions in place or planned. The Current Impact and Likelihood Assessments will provide an accurate reflection of risk exposure when the assessment is undertaken, with the understanding that this will change as the project progresses. This approach aligns with the constantly evolving, ongoing nature of project activity.
New Project Risks may arise at various stages in the lifecycle; these must be documented and assessed.
Impact and Likelihood assessment criteria for Project Risks can be found at Appendix 3 and 4.

Target Risk Ratings for Project Risks

A Target Risk Rating is documented for each risk; prior to, or at, project closure the risk should have reached the Target Risk Rating. As a project progresses through its lifecycle, risks that were identified at the start should see a reduction in risk exposure or be closed as activities are completed.
Impact and Likelihood assessment criteria for Project Risks at Appendix 3 and 4.

Risk Appetite

Council's Risk Appetite Statement details the current risk appetites for Operational and Key Risks.

Where a Key or Operational Risk is assessed as out of appetite, two courses of action are available:

1. Treatment – take action to reduce risk exposure through additional controls or improvement of existing controls
2. Acceptance – accept that action cannot be taken whether because it is not feasible or affordable – see Risk Acceptance section below for further details

Risk Acceptance

ELT will review Operational Risk acceptances to confirm their agreement with the acceptance. ELT will decide upon acceptance for Key Risks.

Risk acceptances are reviewed on an annual basis by the risk owner, to ensure that any additional action that can be taken to reduce risk exposure is considered and applied where appropriate.

Accepted Risks will continue to be reviewed and assessed on a quarterly basis in their relevant register. Approved Risk Acceptances for both Key and Operational Risks will be reported to the Audit and Risk Committee.

Operational Risk Management

Operational Risks (People, Process, Technology, and External Risks) are documented in Operational Risk Registers owned by each Activity Manager.
Operational Risk Registers are reviewed and updated on a six-monthly basis.
Reviews include:

- Checking and updating, when required, Inherent Impact and Likelihood scoring
- Review of existing controls to confirm their continued appropriateness and performance
- Identification of new or missing controls
- Updating Residual Impact and Likelihood scoring to reflect current risk exposure

Out of appetite risks will require action to be documented to enable a reduction in risk exposure, along with an expected date of completion. Once action has been completed, if the risk score remains out of appetite, a Risk Acceptance must be completed (see above). Risk Acceptances will be reported to the Audit and Risk Committee.
Once reviewed and updated, Operational Risk Registers are used to support and inform the Executive Leadership Team's assessment of Key Risks.
More information can be found in the Operational Risk Management Procedure.

Operational Risk Assessments and Reporting

Owner	Assessment Frequency	Reporting Frequency	Reported When	Reported to	Documented in
Activity Managers (Assessments) Risk and Procurement Manager (Reporting)	Six-monthly	Six-monthly	Out of Appetite	ELT Audit and Risk if accepted	Operational Risk Registers

Project Risk Management

Project Risks are documented by Project Managers within Project Risk Registers.

Project risks are reviewed and updated on a monthly basis.

Where a risk is rated high or very high for a full quarter (3 monthly assessments), details will be reported to the Executive Leadership Team (ELT). ELT may decide to report any such risks to the Audit and Risk Committee for noting, giving due consideration to the size, complexity, and value of the project, and whether a decrease in risk exposure has happened since reporting or is due to occur imminently. Project Managers are responsible for assessing risks and reporting any risks that have been rated high or very high for three consecutive months to the Risk and Procurement Manager for further reporting to ELT.

Project Risks may transfer to Business as Usual (BAU) activity once a project closes. Project Risks cannot be transferred to BAU if they represent ongoing project activity, rather than newly created BAU activity. Project Managers must agree a transfer with the relevant Operational Risk Register owner (Activity Manager).
More detail can be found in the Project Risk Management Procedure and Project Management Framework.

Project Risk Assessments and Reporting

Owner	Assessment Frequency	Reporting Frequency	Reported When	Reported to
Project Managers (Assessments) Risk and Procurement Manager (Reporting)	Monthly	Quarterly	3 consecutive monthly assessments of high or very high	ELT Audit and Risk if required

Key Risk Management

Key Risks are owned by ELT Members. Key Risks can be Strategic, Financial, or Operational. These risks require review by Elected Members in their entirety, whether within or out of appetite.
Key Risks are identified via the following means:

- Discussion with ELT Members
- Suggestion from Elected Members
- Issue Management
- Operational Risk Events (whether isolated or repeated)
- Increased risk exposure noted in Operational Risk Registers
- External events
- Audit reports and recommendations
- Legislative requirements
- Changes to legislation
- Change to activity performed by Council

Key risks are assessed by their owner on a quarterly basis. Key Risk Owners should utilise sources of risk information, as well as knowledge of ongoing activity, in order to accurately assess Key Risks.
The Audit and Risk Committee will agree the risks for their focus which should be presented to the committee each quarter. The Audit and Risk Committee will be presented with the full Key Risk Register on an annual basis.
More information can be found in the Key Risk Procedure.

Key Risk Assessments and Reporting

Owner	Assessment Frequency	Reporting Frequency	Reported When	Reported to	Documented in
Executive Leadership Team (Assessments) Risk and Procurement	Quarterly	Quarterly	Risks for Audit and Risk Committee focus reported whether within or out of appetite	Audit and Risk Committee	Key Risk Register

Manager (Reporting)					

Operational Risk Event Management

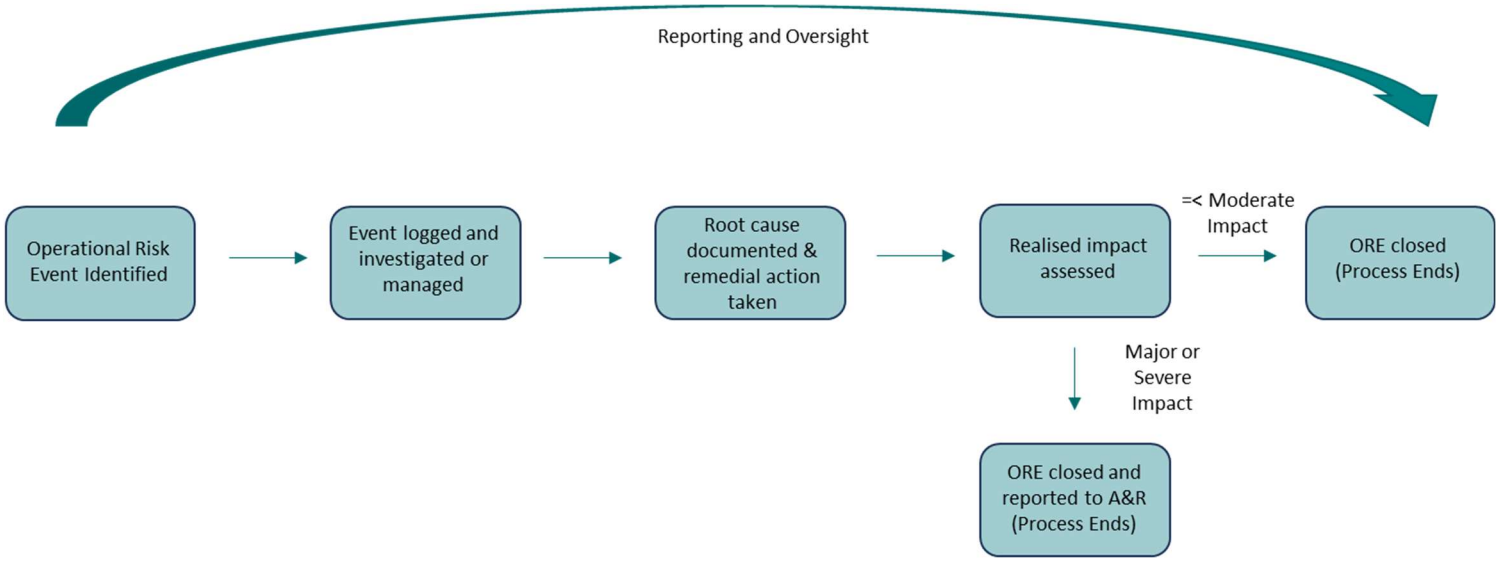
An Operational Risk Event (ORE) is an event that, due to failed or inadequate processes, people or technology, or exposure to external events, results in a loss. Losses may include, but are not limited to:

- Financial Loss;
- Loss of staff;
- Loss of site;
- Loss of reputation;
- Loss of time or resources;
- Loss of supplier; or
- Loss of opportunity.

Operational Risk Events must be investigated by the department in which the event occurred. A root cause must be identified, and any required action documented and undertaken.
In some instances, an event may require ongoing management to ensure resolution, whereas some events may be one-off incidents that need to be retrospectively logged and investigated.
The Risk and Procurement Manager will report open and closed Operational Risk Events to ELT on at least a quarterly basis. Relevant Group Managers will be immediately notified about any ORE with the potential to have a major or severe impact.
When the realised, or actual, impacts of an ORE are understood, these are rated in line with the Impact Assessment Table, found at Appendix 1. Any ORE with an impact of Major or Severe will be reported, following ORE closure, to the Audit and Risk Committee.

More information can be found in the Operational Risk Event Procedure.

Operational Risk Event Reporting Process



Operational Risk Event Process

Process Owner	Reporting Frequency	Reported When	Reported to
Staff (identification and management of events) Risk & Procurement Manager (reporting)	Quarterly	Upon closure of event (once investigated and action taken/planned) that had an impact rated Major or Severe.	ELT Audit and Risk as required

Risk Reporting and Committee Review

As documented throughout this policy, a number of sources of risk information must be reported to the Audit and Risk Committee on a quarterly basis. Once reported, members of the Audit and Risk Committee will review details and have the opportunity to comment on or raise questions about the content of the report. Members of the Audit and Risk Committee should provide oversight to ensure the appropriate management of risk throughout Council.
Information will be provided in a way that best suits the requirements of both Council and Elected Members.

Ongoing Monitoring and Training

Risk management activity will be monitored to ensure adherence to this policy and identify areas for improvement. Risk Management training will be provided to required staff and Elected Members on at least a two-yearly basis.

Glossary

Term	Definition
Risk	A threat to the achievement of objectives. Measured by the combination of impact and likelihood of the risk occurring.
Project Risk	A threat to successful design, implementation, and delivery of a project, or a new risk to Council created by project activity.
Risk Appetite	The level of risk acceptable to an organisation.
Control	Mitigating action to reduce the likelihood or impact of a risk crystalising.
Inherent Likelihood	Score given, in accordance with the risk scoring tables, to represent the likelihood of a risk occurring without any controls in place.
Inherent Impact	Score given, in accordance with the risk scoring tables, to represent the impact of a risk occurring without any controls in place.
Residual Likelihood	Score given, in accordance with the risk scoring tables, to represent the likelihood of a risk occurring after controls have been implemented.
Residual Impact	Score given, in accordance with the risk scoring tables, to represent the impact of a risk occurring after controls have been implemented.
Target Risk Rating	The target score for a project risk to achieve in order for the risk to be closed, or once the project completes.
Operational Risk Event	An event that, due to a risk crystalising through failed or inadequate, processes, systems, people, or an external event, results in a loss.

Related Documents

- Operational Risk Procedures
- Project Risk Procedures
- Key Risk Procedures
- Operational Risk Event Management Procedures

Appendix 1 – Impact Criteria Key and Operational Risks

Impact and Score	Financial Operations	Financial Sustainability	People and Health & Safety	Service Delivery and Assets	Legislative and Regulatory Compliance	Reputation and Relationships	Environment	Systems, data and information
Extreme **5**	Capex overspend of >50% of approved budget Unanticipated costs or losses of > $1 million	Council is unable to obtain an appropriate credit rating, or when holding a credit rating, this is downgraded. Council's long-term financial outlook is extremely poor with results expected to negatively impact the district and ratepayers.	H&S incident resulting in one or more fatalities. Long term severe health effects, including life-changing injuries for one or more individuals. Site shut down, investigation, and notification to Worksafe or other agency. Significantly increased attrition, increased long-term staff absence, and/or significant drop in staff wellbeing.	Key services not available to the majority of the community for over a week. Severe service degradation ongoing for over a month. Critical assets destroyed or rendered unusable for several months.	Breaches result in legal action and/or penalties for Council or officers of Council. Compliance failures result in severe restrictions placed upon two or more areas of core Council business.	National adverse political or media comment. Long-term loss of confidence in Council's capability and standing. New and existing relationships compromised, requiring significant time and effort to repair.	Irreversible and extensive damage to significant natural environments and ecosystems. Widespread irreversible damage to landscapes. Permanent loss of one or more species.	Loss of access to critical systems for over 1 week, non-critical over 2 weeks. Permanent loss of critical data. Data leak/breach of confidential information relating to all Council functions.
Major **4**	Capex overspend of >25% of approved budget Unanticipated costs or losses of $250k - $1m	Council is able to achieve a low credit score that allows low levels of borrowing and shows us as a vulnerable or unattractive borrower. Council's long-term financial outlook is poor.	H&S incident involving multiple casualties requiring hospitalisation. Long-term severe health effects, including life-changing injuries, for an individual. Site shut down, investigation, and notification to Worksafe or other agency. Long-term staff dissatisfaction, slight increase in long-term staff absence, slight increase in attrition, and/or minor drop in staff wellbeing.	Key services not available to a significant portion of the community for less than a week. Severe service degradation ongoing for less than a month. Critical assets rendered unusable for several weeks.	Breaches result in legal action being taken against Council and/or officers of Council. Compliance failures result in substantial restrictions placed on one core Council activity.	Regional adverse political or media comment for more than a week. Loss of confidence in Council's capability and standing lasting several months. New and existing relationships somewhat compromised, requiring additional oversight to improve.	Long-term and significant damage to natural environment and ecosystems taking >5 years to recover and significant restorative work. Localised irreversible damage to landscapes. Long-term reduction in one or more species.	Loss of access to critical systems for less than 1 week, non-critical less than 2 weeks. Data loss/leak of confidential information relating to one Council function.
Moderate **3**	Capex overspend of >10% of approved budget Unanticipated costs or losses of $100k - $250k	Council is able to achieve a lower than desired, but reasonable credit rating. Council's long-term financial stability is negatively impacted, with the outlook less favourable than previously modelled.	H&S incident involving one or more casualties requiring urgent medical attention. Medium-term health effects for one or more people. Investigation and possible site shut down and/or notification to Worksafe or other agency. Medium-term staff dissatisfaction, slight increase in medium-term staff absence.	Key services not available to some of the community for less than a week. Moderate service degradation for less than a month. Multiple non-critical assets rendered unusable for at least a week.	Breaches require significant attention or corrective action. Compliance failures result in restrictions placed upon limited areas of core Council business.	Regional adverse political or media comment for less than a week. Public dissatisfaction lasting from days to weeks. New and existing relationships require increased attention but are not compromised.	Widespread damage to local natural environment and ecosystems taking several years to recover and extensive restoration work. Localised reversible damage to landscapes. Temporary reduction of more than one species.	Loss of access to critical systems for less than 1 day, non-critical less than a week. Data loss/leak of confidential information relating to one Council function.
Minor **2**	Capex overspend of >5% of approved budget Unanticipated costs or losses of $30k - $100k	Council is able to achieve and continue to maintain the desired credit rating. Council's long-term financial stability is called into question, but the outlook remains unchanged.	H&S incident requiring first aider attention resulting in short-term, minor negative health impacts. Internal investigation required, without need for external notification. Short-term staff dissatisfaction, slight increase in short-term staff absence.	Short-term reduced service delivery that does not compromise community outcomes. Small number of non-critical assets unusable for less than a week.	Breach or compliance failure that requires minor remedial action. No restrictions placed on activities.	Local adverse political or media comment for less than a week. Limited dissatisfaction. No impact on new or existing relationships.	Minor damage including temporary pollution or contamination of localised natural environment or ecosystem. Minor reversible damage to landscapes. Temporary reduction of one species.	Loss of access to non-critical systems for less than 1 day. Data loss/leak of non-confidential information relating to more than one Council function.
Insignificant **1**	Opex or capex overspend of less than $30k	Council's short-term stability is impacted, but long-term financial stability is not affected.	H&S incident resulting in momentary or limited health impact. No assistance required. Brief, minor staff dissatisfaction.	Service delivery delays with no negative impact on the community Assets remain in use, but with superficial damage.	Compliance failure that does not result in a breach, with no disruption to performance of duties.	Negative personal views about Council publicly shared with negligible impact on Council's reputation. Public confidence and stakeholder relationships are unaffected.	Brief, non-hazardous and short-term impact on localised natural environment or ecosystem. Minor short-term reversible damage to landscapes	Non-critical systems or data interrupted for less than 4 hours. Data loss/leak of non-confidential information relating to one Council function.

Appendix 2 - Likelihood Criteria Key and Operational Risks

Likelihood	Score	Description
Almost Certain	5	Is expected to occur and is almost inevitable. (occurs once or more in the next 12 months)
Likely	4	Is expected to occur in some circumstances. Not surprised if it happens. (occurs in the next 1-3 years)
Possible	3	Might occur in some circumstances. (occurs in the next 4-10 years)
Unlikely	2	Could occur in some circumstances but would be surprised if it happens. (occurs in the next 11-20 years)
Rare	1	Unlikely to occur but may in exceptional circumstances. It would be highly unexpected. (does not occur in the next 20 years)

Appendix 3 – Impact Criteria (Project Risks)

Impact and Score	Financial - Budget	People and Health & Safety	Timeliness	Legislative and Regulatory Compliance	Scope and Deliverables	Benefits Realisation
Extreme **5**	Capex overspend of >50% of project budget or Unanticipated costs or losses of > $1.5 million	H&S incident resulting in one or more fatalities. Long term severe health effects, including life-changing injuries for one or more individuals. Site shut down, investigation, and notification to Worksafe or other agency. Significantly increased attrition, increased long-term staff absence, and/or significant drop in staff wellbeing.	Delay to project delivery of over 6 months Delays significantly impact ability to progress other key Council deliverables	Breaches result in legal action and/or penalties for Council or officers of Council. Compliance failures result in severe restrictions placed upon two or more areas of core Council business.	Scope or defined deliverables become unviable or inappropriate Project activity negatively impacts the majority of the wider organisation	The majority of key and ancillary benefits fail to be realised Significant impact upon Council's ability to achieve wider objectives
Major **4**	Capex overspend of >30% of project budget or Unanticipated costs or losses of $500k - $1.5m	H&S incident involving multiple casualties requiring hospitalisation. Long-term severe health effects, including life-changing injuries, for an individual. Site shut down, investigation, and notification to Worksafe or other agency. Long-term staff dissatisfaction, slight increase in long-term staff absence, slight increase in attrition, and/or minor drop in staff wellbeing.	Delay to overall project delivery of up to 6 months Delays impact ability to progress other key Council deliverables	Breaches result in legal action being taken against Council and/or officers of Council. Compliance failures result in substantial restrictions placed on one core Council activity.	Elements of scope or defined deliverables become unviable or inappropriate Project activity negatively impacts up to half of the wider organisation	A key benefit fails to be realised Benefits that are realised fail to contribute positively to Council progress of improvement in a measurable way Negative impact on Council's ability to achieve wider objectives
Moderate **3**	Capex overspend of >20% of project budget or Unanticipated costs or losses of $100k - $500k	H&S incident involving one or more casualties requiring urgent medical attention. Medium-term health effects for one or more people. Investigation and possible site shut down and/or notification to Worksafe or other agency. Medium-term staff dissatisfaction, slight increase in medium-term staff absence.	Delays of overall project delivery of up to 3 months Delays impact ability to progress other non-key Council deliverables	Breaches require significant attention or corrective action. Compliance failures result in restrictions placed upon limited areas of core Council business.	Elements of scope or defined deliverables could become less appropriate or feasible. Project activity negatively impacts a small proportion of the wider organisation	Key benefits are not realised, but ancillary benefits are not Benefits that are realised contribute to Council progress to a lesser extent than planned or anticipated
Minor **2**	Operating out of budget but within agreed contingency or Unanticipated costs or losses of $30k - $100k	H&S incident requiring first aider attention resulting in short-term, minor negative health impacts. Internal investigation required, without need for external notification. Short-term staff dissatisfaction, slight increase in short-term staff absence.	Delay to overall project delivery of up to one month Delays do not impact ability to progress other Council deliverables	Breach or compliance failure that requires minor remedial action. No restrictions placed on activities.	Elements of scope or defined deliverables require some change to ensure continued viability and appropriateness Project activity has very little negative impact on the wider organisation	All key benefits are realised and majority of ancillary benefits are realised Benefits that are realised contribute somewhat to Council progress and improvement
Insignificant **1**	Operating close to but within budget Or Unanticipated costs or losses of less than $30k	H&S incident resulting in momentary or limited health impact. No assistance required. Brief, minor staff dissatisfaction.	Delay to achievement of project milestones but on-time project delivery remains viable	Compliance failure that does not result in a breach, with no disruption to performance of duties.	Scope and defined deliverables require insignificant change to ensure continued viability and appropriateness Project has no negative impact on wider organisation	All expected benefits are realised, but to a marginally lesser extent than planned or anticipated

Appendix 4 - Likelihood Criteria (Project Risks)

Likelihood	Score	Description
Almost Certain	5	Is expected to occur and is almost inevitable.
Likely	4	Is likely to occur at least once during project lifecycle. Not surprised if it happens.
Possible	3	Might occur within project lifecycle.
Unlikely	2	Unlikely to occur within project lifecycle. It would be a surprise if it happens.
Rare	1	Highly unlikely to occur at any point in the project lifecycle. It would be highly unexpected.

Appendix 5 – Risk Matrix

Likelihood	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Extreme (5)
Almost Certain (5)	Low (5)	Medium (10)	High (15)	Very High (20)	Very High (25)
Highly Likely (4)	Low (4)	Medium (8)	High (12)	High (16)	Very High (20)
Possible (3)	Low (3)	Low (6)	Medium (9)	High (12)	High (15)
Unlikely (2)	Very Low (2)	Low (4)	Low (6)	Medium (8)	Medium (10)
Rare (1)	Very Low (1)	Very Low (2)	Low (3)	Low (4)	Low (5)

Impact