COOK SHIRE COUNCIL

RISK MANAGEMENT FRAMEWORK

Table of Contents

1. INTRODUCTION

Risk is inherent in all of Council's business activities, programs, services, projects, processes and decisions. This is not reflective of the leadership or management at Council but is due to the legalistic and compliant environment in which it operates and the diverse range of services that it is statutorily required to deliver to the community.

Risk Management hinges on the removal of traditional barriers and divisions to consider risk, not just as involving a loss, but as an event that may provide opportunities which may have both positive and negative consequences. Accordingly Council is committed to the identification and management of all risks associated with the performance of Council functions and delivery of services and to embed risk management as part of Council's corporate governance to protect its employees, the general public, its assets and environment.

The community also needs to have confidence that Council can deliver services by the successful management and mitigation of risks achieved through the application of "value for money" solutions.

A systematic approach to risk management embodies the management of risks – identifying, assessing and controlling them. Risk management forms the crux of good management practice and effective corporate governance which is essential to ensure decisions are made with sufficient information about risks and opportunities.

Through the identification of risks, the organisation is pinpointing any threats or opportunities that impinge on its strategic goals and objectives. Informed decisions need to be made whether to accept, transfer or mitigate risk in the context of achieving strategic goals and objectives.

The Cook Shire Council Risk Management Framework should be read and administered in conjunction with *ISO 31000:2018 Risk Management - Guidelines* and Cook Shire Council's Risk Management Policy.

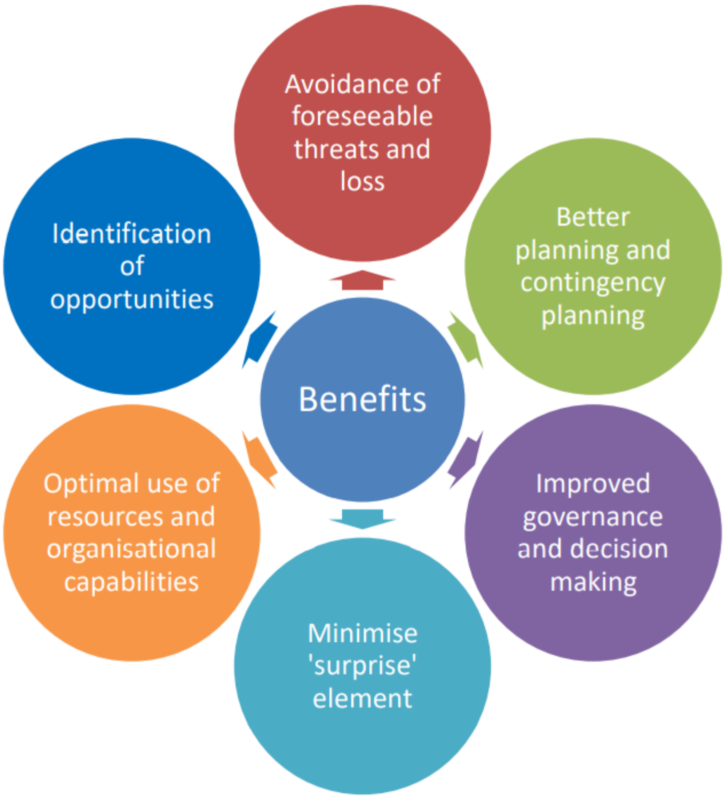
2. PURPOSE

The purpose of this framework is to provide a consistent organisation-wide approach to risk management through clear guidance and instructions on how to manage risks. This is achieved by explaining how risks are identified, assessed, treated and reported throughout the organisation.

The Framework also aims to:

- Determine the level of risk Council is prepared to accept;
- Develop and promote a positive risk management culture, integrated throughout Council as part of the day-to-day business and organisational activities;
- Develop proactive strategies to identify, control, treat and manage risks;
- Establish organisational roles, responsibilities and accountabilities for managing risk;
- Strengthening sound corporate governance practices, supporting informed decision making, priority planning, budgeting and reporting;
- Facilitate continual improvement and enhancement of Council's processes and systems including periodic review of risks;

The successful implementation of a proactive risk culture throughout the organisation will derive tangible benefits to the ongoing viability and sustainability of Council. These benefits are depicted in the following diagram:


Benefits
Avoidance of foreseeable threats and loss
Better planning and contingency planning
Improved governance and decision making
Minimise 'surprise' element
Optimal use of resources and organisational capabilities
Identification of opportunities

3. DEFINITIONS

Risk	A risk to the business is any action or event that has the potential to impact on the achievement of our business objectives. Risk also arises as much from the possibility that opportunities will not be realised as it does from the possibility that threats will materialise or that errors will be made.
Risk Management	Risk management for Council refers to the culture, processes and structures developed to effectively manage potential opportunities and adverse effects for any activity, function or process undertaken by the Council. Managing risk is achieved through the systematic application of policies, procedures and practices to identify, analyse, evaluate, treat, monitor and communicate risk.
Enterprise Risk Management (ERM)	Enterprise Risk Management encompasses all the major risk categories (including financial, environmental, health and safety, fraud, information technology, compliance, security and business continuity) and includes the coordination, integration, consolidation and consistency of reporting by the various Council functions with identified risks.
Risk Register	A list of identified and assessed risks directly related to either a particular directorate or to the whole of Council. Risk Registers can be held at either Corporate, Operational, Project or Event level.
Likelihood	The chance of something happening, whether defined, measured or determined objectively or subjectively (probability or frequency).
Consequence	The outcome of an event affecting objectives (impact/magnitude). An event can lead to a range of consequences. A consequence can be certain or uncertain and can have a positive or negative effect on objectives. Consequences can be expressed qualitatively or quantitatively.
Risk Owner	The person with the accountability and authority to manage a risk. The owner may delegate some duties in relation to managing the risks for which they are responsible, however they are ultimately accountable for the risks allocated to them.
Risk Treatment	The process of selecting and implementing measures that will assist in the mitigation of an identified risk to reduce adverse impacts on business operations.
Risk Treatment Action Plan	The document that outlines the steps to be taken to reduce unacceptable risks to achievable and acceptable levels. This includes details on current controls; required risk treatments; improvement opportunities; resources; timing; reporting and accountabilities. Action Plans must be reviewed on a regular basis to ensure controls are actually working.

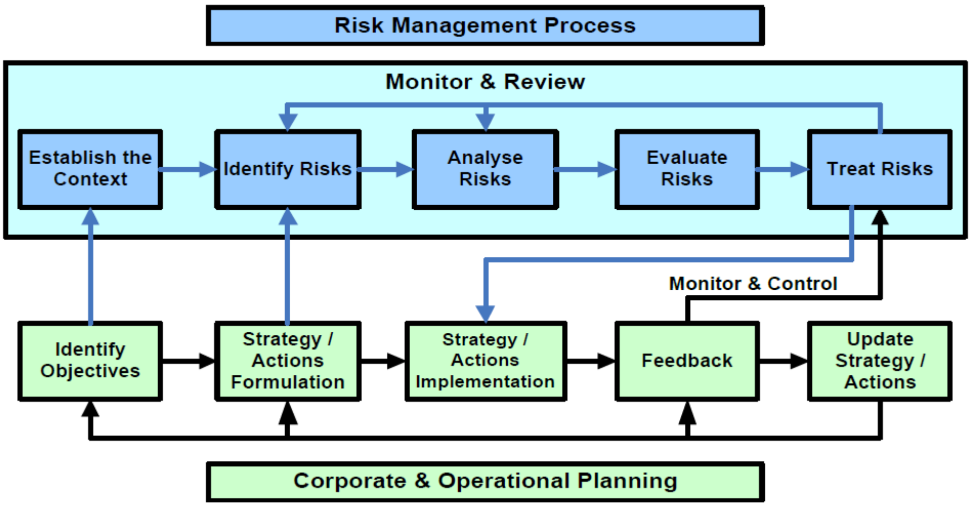
4. RISK MANAGEMENT PRINCIPLES

To build an effective risk management culture throughout the organisation, this framework has been developed based on the following principles which have been adapted from *AS/NZS ISO 31000:2018 Risk Management - Guidelines*:

- **Integrated** - risk management is an integral part of all organisational activities;
- **Structured and comprehensive** - a structured and comprehensive approach to risk management contributes to consistent and comparable results;
- **Customised** - the risk management framework and process are customised and proportionate to the organisation's external and internal context related to its objectives;
- **Inclusive** - Appropriate and timely involvement of the stakeholders enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management;
- **Dynamic** - Risk can emerge, change disappear as an organisation's external and internal context changes. Risk management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner;
- **Best available information** - The inputs to risk management are based on historical and current information, as well as on future expectations. Risk management explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders;
- **Human and cultural factors** - Human behaviour and culture significantly influences all aspects of risk management at each level and stage;
- **Continual improvement** - Risk management is continually improved through learning and experience.

5. RISK MANAGEMENT FRAMEWORK

Management will use the Risk Management Framework in determining the risks associated with achieving corporate plan outcomes and operational plan key performance indicators, thereby supporting and facilitating the achievement of corporate goals and objectives. The following diagram illustrates the process:



6. RESPONSIBILITIES

The embedding of a risk management culture in all Council operations is the responsibility, jointly and separately, of Council, Executives, Managers and employees. Further details on responsibilities are detailed in the table below:

Responsible Officer	Responsibility
Council	• In accordance with the principle of good governance under the *Local Government Act 2009*, Council has the responsibility to prudently manage risks and ensure staff can supply all necessary information to enable effective decision making • Adoption of Risk Management Policy and Risk Management Framework • With the assistance of the Executive Leadership Team, manage Council's strategic risks and the effectiveness of risk treatments and controls
Audit and Risk Committee	• Providing oversight and advice to Council on strategic issues and promote sound risk management practices throughout Council • Contribute to the review of processes ensuring a consistent approach is taken in the management of risk across Council • Monitor the review of Risk Registers on a periodic basis and advise on the adequacy of control measures • Facilitate an alignment of internal audit plans to data and information arising from risk assessments
Executive Leadership Team	• Implement, embed and maintain a risk management culture within the organisation through advocacy, leadership and mandate • Ensure the risk management processes are integral to Council operations to enable realisation of corporate goals and objectives • Capitalise on opportunities as they arise through risk identification • Ensure that Risk Owners undertake regular review of risks and proactively identify new risks • Report regularly on the level, treatment and management of risks ensuring the accuracy and validity of risk information reported • To the best of their ability, ensure sufficient resources are available to effectively manage risks
Managers and Risk Owners	• Responsible to their Director for the risk management function within their area of responsibility • Strongly advocate and support a risk management culture • Continually identify, assess and manage risks relevant to their area of responsibility • Ensure all risk reviews and subsequent reporting is undertaken in a timely manner
Staff	• Ensure they fully support their Managers and Risk Owners identify, assess and control risks pertinent to their work areas

7. RISK MANAGEMENT PROCESS

The Council risk management process is designed to facilitate evidence-based decision making around matters concerning risk management. A robust approach is applied that focuses on the use of risk assessments in a consistent manner and the use of common language consistent with *ISO 31000:2018 Risk Management - Guidelines.*

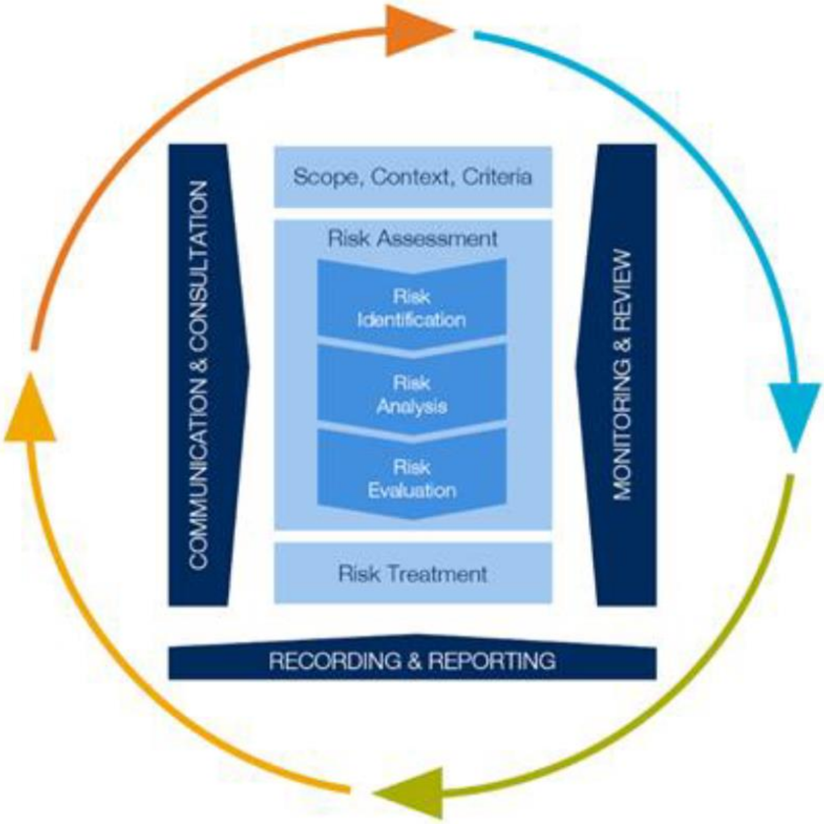
The risk management process must be an integral part of management, embedded in the culture and practices of Council and tailored to Council's operational and business processes.

This process is the application of the structured risk management methodology to be used to assess; prioritise; treat and monitor risks identified. The risk management process may capture inherent risk (prior to taking into account controls in place), residual risk (after taking into account controls in place), or both.

The main elements of an effective risk management approach are as follows:

- Communicate and Consult
- Establish the Context
- Risk Assessment
    - o Identify Risks
    - o Analyse Risks
    - o Evaluate Risks
- Treat Risks
- Monitor and Review

The following diagram represents the components of the risk management process. Each of these components are explained further below.



COMMUNICATE AND CONSULT

It is an essential part of the risk management process to develop and implement an effective framework to communicate and consult with all relevant stakeholders, internal and external as appropriate, at each stage of the risk management process and concerning the process as a whole.

The level of communication and consultation will vary depending on the level of interest and or influence of that particular stakeholder individual or group. Communication and consultation are necessary at every stage of the risk management process.

SCOPE, CONTEXT, CRITERIA

In the initial stage of the risk management process, it is imperative to establish the scope, context and criteria as this will inform the rest of the process which is to follow.

Scope: The scope of risk management is to be applied to all level of risks that cover Council operations including strategic, operational, programs, projects, events and any other activities.

Context: The context assesses both the external and internal environment in which Council operates and is to reflect the specific environment to which the risk management process is to be applied.

Criteria: The criteria is to establish the level and type of risk Council is prepared to accept to achieve objectives and to also evaluate the significance of risk and to support decision making processes.

RISK ASSESSMENT - IDENTIFICATION

The risk identification process includes identifying sources of risks as well as their causes, together with the relevant circumstances which can impact on goals and objectives and the nature of that impact. This is undertaken at both the strategic and operational level of Council.

Risk identification can often be simplified to two basic questions:

- what can happen; and
- how might it happen.

RISK ASSESSMENT - ANALYSIS

This stage determines the inherent risks and then calculates any residual risks taking into consideration any existing controls in place (existing processes and procedures).

Risks are analysed in terms of consequence and likelihood in the context of those controls. The analysis will consider the range of potential risk exposure consequences and how likely those consequences are to occur. The Consequence and Likelihood are then combined to produce an estimated level of risk known as the Overall Risk Rating.

Determining Likelihood

In determining the likelihood of each risk, the following ratings and definitions have been applied. In making your assessment you have to remember that some events happen once in a lifetime, others can happen almost every day. Judgement is required to determine the possibility and frequency that the specific risk is likely to occur.

Description	Definition - Likelihood of Occurrence
Rare	Event may occur once in every 10+ years
Unlikely	Event may occur once in every 5 – 10 years
Possible	Event may occur once in every 2 – 5 years
Likely	Event may occur once in every 1 – 2 years
Almost Certain	Event may occur within one year

Determining Consequence

In determining the consequence of each risk, the following ratings and definitions have been applied. There are five levels used to determine consequence and when considering how risks may impact on the organisation it is also important to think about the non-financial elements as well.

Description	Qualitative Definition - Consequence
Insignificant	An event, that impact can be absorbed; no injuries; low financial loss
Minor	An event, the consequences of which can be absorbed but management effort is required to minimise the impact; first aid treatment; low-medium financial loss
Moderate	A significant event, which can be managed under normal circumstances; medical treatment; medium financial loss
Major	A critical event, which with proper management can be continued; extensive injuries; loss of production capability; major financial loss
Catastrophic	A disaster, which could lead to the collapse of the organisation; death; huge financial loss

Quantitative parameters have been developed to enable Council to consistently assign consequence ratings to potential risks. These quantitative measures assign the organisation's risk tolerance parameters applicable to each of the five consequence levels. This approach ensures that all staff can rate the consequence of a risk occurring against the organisation's established parameters, instead of their own personal choice.

Consequence	Financial (Revenue & Costs)	Information Technology & Data	Infrastructure Assets/Property	Environment	Operational – Business Continuity	Strategic/Corporate Governance- Reputation – Political	Workplace Health & Safety	Legal Compliance, Regulatory & Liability
Catastrophic	Huge financial loss. >$500K	Extensive loss of/damage to assets and/or infrastructure. Permanent loss of data. Widespread disruption to the business.	Widespread substantial/permanent damage to assets and/or infrastructure.	Long-term large scale damage to habitat or environmental. Serious/repeated breach of legislation/licence conditions. Cancellation of licence and/or prosecution.	The continuing failure of Council to deliver essential services. The removal of key revenue generation.	Loss of State Government support with scathing criticism and removal of the Council. National media exposure. Loss of power and influence restricting decision making and capabilities.	Fatality or significant irreversible disability.	Extensive breach involving multiple individuals. Extensive fines and litigation with possible class action. DLG review or Administrator appointed
Major	Major financial loss. >$150K to <$500K	High risk of loss/corruption of data; significant catch-up will be required. Business continuity plans should be implemented.	Significant/permanent damage to assets and or infrastructure.	Severe impact requiring remedial action and review of processes to prevent re-occurrence. Penalties and/or directions or compliance order incurred	Widespread failure to deliver several major strategic objectives and service plans. Long-term failure of Council causing lengthy service interruption.	State media and public concern/exposure with adverse attention and long-term loss of support from Council residents. Adverse impact and intervention by State Government.	Extensive injuries. Lost time of more than 4 working days.	Major breach with possible fines or litigation. DLG or Administrator may be involved. Critical failure of internal controls, may have signification and major financial impact
Moderate	High financial loss. >$50K to <$150K	Moderate to high loss of IT. Some data may be permanently lost. Workarounds may be required.	Moderate to high damage requiring specialist/contract or equipment to repair or replace.	Moderate impact on the environment; no long term or irreversible damage. May incur cautionary notice or infringement notice.	Failure to deliver minor strategic objectives and service plans. Temporary & recoverable failure of Council causing intermittent service interruption for a week.	Significant state wide concern/exposure and short to mid-term loss of support from Council residents. Adverse impact and intervention by another local government & LGAQ	Medical treatment. Lost time of up to 4 working days	Serious breach involving statutory authorities or investigation. Prosecution possible with significant financial impact. Possible DLG involvement. Moderate impact of legislation/regulations.
Minor	Minor financial loss. >$20K to <$50K	Minor loss/damage to IT and communications. Some data catch-up may be required.	Minor loss/damage. Some repairs may be required.	Minor localised impact; one-off situation easily remedied.	Temporary and recoverable failure of Council causing intermittent service interruption for several days.	Minor local community concern manageable through good public relations. Adverse impact by another local government.	First aid treatment. No lost time	Minor breach with no fine or litigation. Contained non-compliance or breach with short term significance with minor impact. Some impact on normal operations.
Insignificant	Low financial loss. $0 to <$20K	Negligible loss or damage to IT hardware and communications. No loss of data.	Negligible damage to or loss of assets.	Minor breach of environmental policy /practices. Negligible impact on the environment	Negligible impact of Council, brief service interruption for several hours to a day.	Transient matter, e.g. Customer complaint resolved in day to day management. Negligible impact from another local government	No injury	Isolated non-compliance or breach. Minimal failure managed by normal operations. Insignificant legislation/regulations.

Determining the Overall Risk Rating

After the consequence and likelihood ratings have been determined they are combined in a matrix to determine the overall risk rating for each risk. The extent of the consequences and the extent of the likelihood risks will be assessed using a scale containing Low, Moderate, High and Extreme.

The table below illustrates how the combination of the consequence and likelihood generates the overall risk rating.

Likelihood	Consequence				
	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	M	H	H	E	E
Likely	M	M	H	H	E
Possible	L	M	H	H	H
Unlikely	L	L	M	M	H
Rare	L	L	M	M	H

RISK ASSESSMENT - EVALUATION

Risks need to be evaluated and prioritised to ensure that management effort is directed towards resolution of the most significant organisational risks first. The initial step in this Risk Evaluation stage is to determine the effectiveness, and or existence of, controls in place to address the identified risks.

The following table will assist to determine the effectiveness, and or existence of, controls in place to address the identified risks.

Control Assessment	Description
Adequate	• The controls address the identified risk and there is little scope for improvement. • There is no convincing cost/benefit justification to change the approach.
Opportunities for Improvement	• The controls contain some inadequacies and scope for improvement can be identified. • There is some cost/benefit justification to change the approach.
Inadequate	• The controls do not appropriately address the identified risk and there is an immediate need for improvement actions. • There is a significant cost/benefit justification to change the approach.

RISK TREATMENT

After evaluating each risk and appropriate controls, it is the responsibility of the manager to implement the suitable treatment. Treatment needs to be appropriate to the significance and priority of the residual risk. As a general guide:

a) **Control the risk** – by either reducing the likelihood of occurrence or the consequences e.g. implement procedures for specified tasks.

b) **Retain the risk** – where the risk cannot be avoided, reduced or transferred. In such cases, usually the likelihood and consequence are low. These risks should be monitored, and it should be determined how losses, if they occur, will be funded.

c) **Transfer the risk** – involves shifting all or part of the responsibility to another party who is best able to control it (such as an insurer who bears the consequence of losses e.g. Motor vehicle insurance for Council vehicles).

d) **Avoid the risk** – decide not to proceed with the policy, program or activity or choose an alternative means of action.

Determine the most effective treatment options by considering the:

- Cost/benefit of each option including the cost of implementation (do not consider financial considerations only; organisational, political, social and environmental factors should also rank)
- Use of proven risk controls
- Anticipated level of risk remaining after implementation of risk treatment. The final acceptance of this risk will be a matter for the appropriate Director to decide.

Once treatment options for individual risks have been selected, they should be assembled into action plans, risk treatment plans or strategies. The outcome of an effective risk treatment plan is knowledge of the risks Council can tolerate and a system that minimises those risks that it cannot tolerate.

The decision to accept a risk will be determined by the agreed table indicating proposed corrective action and the risk appetite criteria established by the Council. The approach for treatment of risks is:

Risk Level	Appropriate Management Response
Extreme	**Needs Active Management:** A risk action plan must be established and implemented
High	**Needs Regular Monitoring:** Existing good controls should be maintained and any additional risk actions required should be defined and implemented
Moderate	**Needs Periodic Monitoring:** Risk should be monitored in conjunction with a review of existing control procedures
Low	**No Major Concern:** Significant management effort should not be directed towards these risks

MONITORING AND REVIEW

This stage establishes a process to monitor and review the performance of the risk management system implemented and changes that might affect the performance or give rise to new risks that will require assessment.

Both monitoring and reviewing should be a planned part of the risk management process and tailored to the needs of the organisation and the significance of the risks identified. It should be undertaken on at least an annual basis.

The continual process of monitoring and reviewing is required to ensure ongoing effective risk treatments and the continual improvement of the risk management standards.

Monitoring – assess whether current risk management objectives are being achieved. Council can use inspections, incident reports, self-assessments and audits to monitor its risk management plan.

Review – assess whether the current risk management plan still matches Council's risk profile. The risk management plan may be reviewed by studying incident patterns, legislative changes and organisational activities.

Possible methods for review:

- Internal check program/audit or independent external audit;
- External scrutiny (appeal tribunal, courts, commission of inquiry);
- Physical inspection;
- Program evaluation; and
- Reviews of organisational policies, strategies and processes.

When completing the review process, it is important the context in which the original risk was developed is reassessed. The review should also be informed by reports and recent events and include consideration of:

- Completeness of the register;
- Continued existence of controls;
- Adequacy of controls;
- Risk ratings;
- Treatment strategies;
- Risk owner; and
- Risk review date.

RECORDING & REPORTING

Each stage of the risk management process must be recorded appropriately. All risk assessments and Risk Treatment Action Plans must be documented, retained and easily accessible for future reference. Even if a risk is assessed to be low and a decision is taken to do nothing, the reasoning that led to the decision must be recorded.

8. RISK REGISTER

Two Risk Registers have been developed, Strategic Risk Register and Operational Risk Register, to record and assess each risk as part of the risk identification stage.

The application of the stages of the risk assessment process noted above ensure there is consistency in the determination of the current risk severity level, taking into account the existing controls and their level of effectiveness in mitigating or addressing the risk.

9. COMMUNICATION

The Risk Management Policy, Framework, Risk Registers and associated documents and procedures will be held in Council's Electronic Document and Records Management System (EDRMS) and will be accessible to stakeholders according to their authority levels.

The existence of all relevant risk management documentation will be shared with staff at all levels to encourage their awareness of how the organisation is managing its risks.

Following reviews of the Risk Management Policy and Framework, any changes will be communicated to the relevant Risk Owners and other stakeholders to ensure that the risk management process remains dynamic and relevant.

10. REVIEW

To ensure that the focus of risk management remains an integral component of Council's operations and corporate governance functions the following review cycle has been implemented:

Item/Matter	Process
Risk Management Policy	The policy is to be reviewed every two years or where there is a major change in Council. Policy will be presented to the Audit & Risk Committee for endorsement prior to adoption by Council.
Risk Management Framework	The framework is to be reviewed every two years or when improvements have been identified. Framework will be presented to the Audit & Risk Committee for endorsement prior to adoption by Council.
Risk Management Process	The risk management function and processes will be monitored and reviewed on an ongoing basis with any changes being approved by the Executive Leadership Team. As and when deemed appropriate these changes will be communicated to the Audit & Risk Committee.
Strategic Risks	The Executive Leadership Team, in conjunction with Councillors, to review all strategic risks and extreme operational risks and their treatments. This review is to occur on at least an annual basis and the outcomes of this review to be reported to the Audit & Risk Committee.
Operational Risks	Directors, Managers and Risk Owners are responsible for reviewing operational risks and the relevance of the treatments applied. This review is to occur on at least an annual basis and the outcomes of this review to be reported to the Executive Leadership Team and subsequently to the Audit & Risk Committee.

9. RELATED DOCUMENTS

- *AS/NZS ISO 31000:2018 Risk Management – Guidelines*
- Cook Shire Council Corporate Plan
- Cook Shire Council Risk Management Policy
- *Local Government Regulation 2012* (in particular S164)