Enterprise Risk Management Framework

Policy Type	Council Framework	Version:	3
Responsible Officer	Manager Development and Governance	Date Approved:	19/06/2024
Review Officer:	Director Corporate and Community Services	Review Due:	19/05/2026
Author:	Manager Development and Governance	Commencement:	19/06/2024

1. INTRODUCTION

As defined in AS/NZS ISO 31000:2018 - Risk Management - Guidelines, risk is the effect of uncertainty on objective and risk management is the approach encompassing strategy, processes, culture, technology, standards and knowledge in identifying, analysing, evaluating, managing, treating, monitoring, reviewing and communicating uncertainties the organisation encounters. In other words risk management is a suite of 'tools' to identify and mitigate the risk of uncertainty in meeting Council's strategic and operational objectives.

However, enterprise risk management is more than risk management. Enterprise risk management (ERM) is a structured, coordinated approach of aligning strategy, processes, people, technology and knowledge to manage risk.

While risk is inherent in all of Council's business activities, programs, services, projects, processes and decisions, enterprise risk management is about removing traditional divisions or barriers and including thinking about risk, not just as involving a loss, but as an occurrence that may provide opportunities which may have both positive and negative consequences. As such, Council is committed to consistent, efficient and effective risk management, sharing risk information across the organisation to allow effective allocation of resources and reduced duplication.

Enterprise risk management requires the Council and management to consider the bigger risk landscape and the processes that flow from this; noting that risk management is the responsibility of Council, Council employees, contractors, volunteers and suppliers.

This Enterprise Risk Management Framework should be read in conjunction with the Enterprise Risk Management Policy and the Enterprise Risk Management Process. The implementation of this framework will:

- ensure a consistent and best practice approach to risk management throughout the organisation;
- establish a structured process for identifying, analysing, evaluating, managing, treating, monitoring, reviewing and communicating risks; and
- encourage the integration of risk management into Council's overall governance, planning, management, reporting processes, policies, operations, values and culture.

1.1 COUNCIL'S MISSION

Provide cost-effective services, foster collaborative partnerships and maintain accountable governance to promote the prosperity and liveability of the Shire.

1.2 COUNCIL'S VALUES

Council has established a set of values which are implicit in our work practices, including risk management, and guide us in servicing our community. Corporate Values and Principles are;

1. **Sustainable**
   We operate in an efficient and effective businesslike manner to ensure long-term sustainability by optimising customer service levels whilst managing community expectations.

2. **United team**
   Our people work respectfully and collaboratively to achieve Council's goals with every decision being made based on what is best for the whole organisation.

3. **Customer focussed**
   The community are our customers and we are here to serve our community in everything we do.

4. **Community Partnerships**
   We build partnerships with the community to deliver better outcomes.

5. **Ethical Conduct**
   We operate fairly, with open, honest, transparent and accountable behaviour and consistent decision-making.

6. **Striving to be better**
   We strive to improve Council's service and enthusiastically pursue innovative ways of providing services simply and effectively.

7. **Skilled workforce**
   We ensure our workforce is equipped with the skills and knowledge needed for today and into the future.

1.3 ERM FRAMEWORK INTEGRATION WITH THE CORPORATE PLAN

The Enterprise Risk Management Framework aims to enhance Council's ability to meet its corporate and operational objectives. Figure 1 shows how the strategic and operational planning process is integrated and linked to the risk management process.

Our corporate objectives are:

Financial Sustainability - A council that continuously operates in a cost-effective manner while managing council's assets and reserves to ensure a sustainable future.

Community - An informed and engaged community which supports and encourages effective partnerships to enhance the liveability of the shire.

Transport and Council Infrastructure - The provision of quality services and infrastructure for our growing community that is planned and managed using sound asset management principles.

Economy and Environment - A resilient economy that promotes and supports the shire's natural assets and local industry and encourages investment while preserving and future proofing for generations to come.

Governance - Sound decision making based on effective frameworks and clear strategic direction to achieve regulatory compliance while delivering affordable levels of identified services within the Shire.

Management will use the Enterprise Risk Management Framework in determining the risks associated with achieving the corporate plan activities and operational plan key performance indicators; thereby using enterprise risk management (ERM) to support and facilitate the achievement of our strategic and operational objectives.

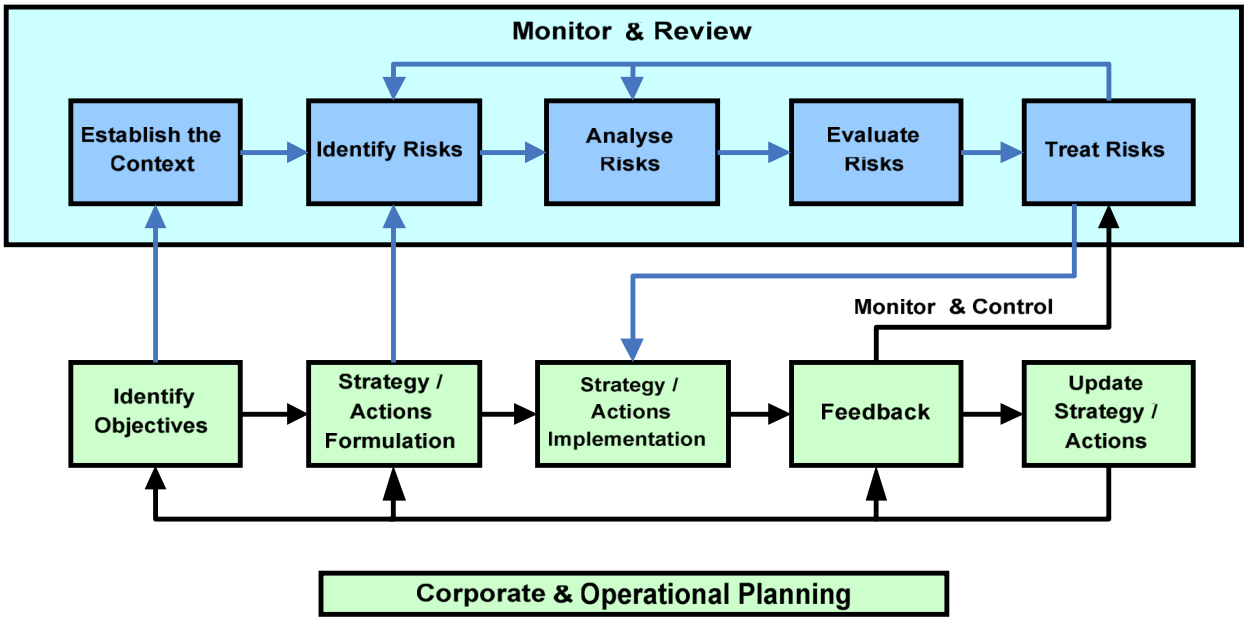

Figure 1 - Linking Corporate and Operational Planning with Risk Management

2. PURPOSE

The purpose of the Enterprise Risk Management Framework is to provide an organisational approach towards the management of risk. ERM encompasses the following:

- Application of the level of risk Council is prepared to accept.
- Development of proactive strategies to identify, control, treat and manage those risks.
- Developing and promoting a positive risk management culture, integrated throughout Council as part of the day-to-day business and organisational activities.
- Strengthening sound corporate governance practices, supporting informed decision making, priority planning, budgeting and reporting.
- Improving operational effectiveness and efficiency, and communication of risk throughout the organisation.
- Establishment of organisational roles, responsibilities and accountabilities for risk management.

3. RELATED DOCUMENTS

- *AS/NZS ISO 31000:2018 Risk Management – Guidelines*
- *Corporate Plan* (MSC)
- *Enterprise Risk Management Policy* (MSC)
- *Enterprise Risk Management Process* (MSC)
- *Fraud and Corruption Control Policy* (MSC)
- *Fraud and Corruption Control Plan* (MSC)

- *Local Government Regulation 2012* (Qld)
- *Operational Plan* (MSC)

4. DEFINITIONS

For the purposes of this framework the following definitions apply:

CEO	Chief Executive Officer A person who holds an appointment under section 194 of the Local Government Act 2009. This includes a person acting in this position.
Control Owner	The person responsible for implementing controls and monitoring existing controls to determine, document and report on control effectiveness, adequacy and changes in risk environment. In some cases the control owner is the risk owner or the control owner would normally report to the risk owner.
Council	Mareeba Shire Council.
Council ERM Standards	Rules providing instruction to risk owners and Council employees on specific areas of their risk management responsibilities.
Current (Residual) Risk Rating	The level of risk remaining after risk treatment.
Enterprise Risk Management (ERM)	Council's approach to risk management encompassing strategy, processes, culture, technology, standards and knowledge in identifying, analysing, evaluating, managing, treating, reviewing and communicating uncertainties encountered to achieve an appropriate balance between minimising losses and maximising opportunities in meeting its objectives.
Enterprise Risk Management Framework	Council's adopted systems, processes and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving ERM throughout Council. The framework provides an expression of intent on what, why and how risk is to be managed and shows how Council provides capacity to manage risk according to the intent.
Risk	The effect of uncertainty on objectives.
Risk Analysis	A process of identifying the cause and source of a risk, its positive and negative consequences, and the likelihood that those consequences can occur. The level of risk is determined through this process.
Risk Calculator	A tool for ranking and displaying risks by defining ranges for consequence and likelihood.
Risk Criteria	Terms of Reference against which the significance of a risk is evaluated. Risk criteria are based on organisational objectives, internal and external context and can be derived from standards, laws, policies and other requirements.
Risk Owner	A Council employee (usually a Director and/or Manager) authorised by the CEO to manage a particular risk and is accountable for doing so.
Risk Profile	Description of any set of risks as defined. For example: the whole of council or only a part.
Risk Register	The system maintained by Council listing the identified and assessed risks.
Risk Tolerance	Organisation's or stakeholder's readiness to bear the risk, after risk treatment, in order to achieve its objectives.
Risk Treatment	The process to modify risk. Can involve taking (opportunity), avoiding, removing, changing, sharing. If the risk has a negative consequence treatment may also be referred to as risk mitigation.

Risk Treatment Plan	A plan detailing the process to modify risk.
Senior Management Team	For the purpose of implementing the ERM framework this refers to the CEO, Directors, Managers and other employees approved by the CEO to be a risk owner.

5. RISK MANAGEMENT PRINCIPLES

This ERM framework is based on the following risk management principles as adapted from AS/NZS ISO 31000:2018 - Risk Management - Guidelines:

a) Integrated - risk management is integral part of all organisational activities;

b) Structured and comprehensive - a structured and comprehensive approach to risk management contributes to consistent and comparable results;

c) Customised - the risk management framework and process are customised and proportionate to the organisation's external and internal context related to its objectives;

d) 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;

e) 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;

f) 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;

g) Human and cultural factors - Human behaviour and culture significantly influences all aspects of risk management at each level and stage;

h) Continual improvement - Risk management is continually improved through learning and experience;

6. RESPONSIBILITIES

The imbedding of a risk management culture in all work and business practices within the organisation is the responsibility of Council, Council employees, contractors, volunteers and suppliers. The responsibilities and accountabilities of specific personnel or groups of personnel are shown in Figure 2 and described below:

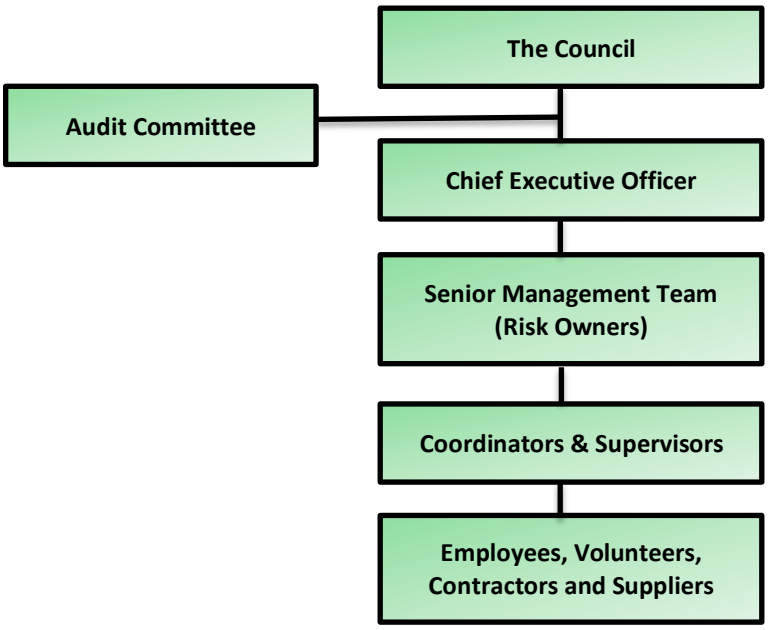

Figure 2 - ERM Governance Structure

6.1 THE COUNCIL

The Council provides direction and oversight of risk management across the organisation including:

- Adoption of Council's ERM Policy, this framework, risk registers and any updates. These ordinarily will be first reviewed by Audit Committee if the timing of their meetings allows for it;
- Oversee the management of risks with a high or very high current risk rating, including the effectiveness of associated controls through the review and discussion of quarterly risk management reports;
- Satisfying itself that the **a**s **l**ow **a**s **r**easonably **p**racticable (ALARP) evaluation of risks with an existing high or very high current risk rating is tolerable;
- Satisfying itself that risks with lower ratings are effectively managed, with appropriate controls in place and effective reporting structures; and
- Approving major decisions affecting Council's risk profile or exposure.

6.2 CHIEF EXECUTIVE OFFICER (CEO)

The CEO is accountable to the Council and has overall responsibility for protecting the organisation from unacceptable costs or losses associated with Council operations and for developing, approving and implementing processes for effectively managing the risks that may affect the achievement of Council's corporate and operational objectives-specifically Council's ERM framework, policies and process.

6.3 SENIOR MANAGEMENT TEAM

The effectiveness of ERM within Council is directly linked to management's awareness of and commitment to its principles and the promotion and application of risk management in decision making and day-to-day operations.

The Senior Management Team, as the risk owners within their areas of responsibility, is responsible for:

- Promoting and overseeing the development of a positive risk management culture throughout Council;
- Providing direction and guiding the inclusion of risk management in all corporate and operational decision making;
- Possessing a clear understanding of the risk profile relating to their area;
- Maintaining the framework for managing, monitoring and reporting risk;
- Performance against the risk register. This will be a key performance indicator and will be assessed as applicable;
- Documenting any new risks identified due to changes in the work environment. Risk records must be maintained and updated on an on-going basis to reflect any changes;
- Having an appreciation of the wider risk environment and where risks extend beyond their direct control, cooperating to identify and prioritise risks, developing clear accountabilities for their management and committing to collective solutions and outcomes. Where risks may impact across another risk owner's area of responsibility, collaborating with the appropriate employees to ensure that the risk is being adequately managed, e.g. the risk isn't being over or under controlled; and
- Ensuring adequate resourcing and risk management training in their area.

6.4 COORDINATORS AND SUPERVISORS

Applicable to their area of responsibility, Coordinators and Supervisors are responsible for the implementation of risk management practices (e.g. internal controls) and the results of those activities.

6.5 ALL EMPLOYEES, VOLUNTEERS, CONTRACTORS AND SUPPLIERS

All Council employees, volunteers, contractors and suppliers are responsible for:

- Meeting their obligations under relevant legislation (including Workplace Health and Safety) and the ERM framework;
- Acting at all times in a manner which does not jeopardise the health and safety of themselves or any other person in the workplace;
- Providing direction and training to persons for whom they have a supervisory responsibility or duty of care provision relating to risk management, and health and safety;
- Identifying areas where risk management practices should be implemented and documented, advising their supervisors accordingly; and
- Reducing the risk, and minimising the impact, of fraud and corruption within their work environment.

6.6 AUDIT COMMITTEE

The main objective of the Audit committee is to assist Council in fulfilling its corporate governance role and oversight of financial management and reporting responsibilities imposed under the Financial and Performance Management Standard 2009, the Queensland *Local Government Act 2009* and other relevant legislation. More specifically, the Committee will:

- Enhance Councillors' ability to exercise due care, diligence and skill in relation to compliance with applicable laws and policy;
- Provide advice to Council (via Audit Committee) to allow Councillors confidence that processes and procedures within the organisation are appropriate and being managed properly;
- Monitor the credibility and objectivity of financial reports;
- Ensure the independence and effectiveness of Council's Internal Audit function;
- Monitor the use of appropriate accounting and disclosure policies;
- Maintain its independence from the day-to-day operation of the Council;
- Monitor existing corporate policies and recommend for consideration any new corporate policies it considers necessary to prohibit unethical, questionable or illegal activities;
- Advise Council regarding its management of its strategic risks;
- Support measures to improve internal controls and the minimisation of risks and fraud.

7. COUNCIL'S ERM STANDARDS

The following standards are provided to support ERM and to provide clear instruction to risk owners on the approach Council requires.

7.1 STANDARD 1 - SUPPORT AUDIT RECOMMENDATIONS

Risks identified through either an internal or external audit shall be placed in the appropriate risk register by the risk owner (the Manager Development & Governance can assist if required). The final content of the documented risk and any risk treatment plan is the responsibility of the risk owner.

7.2 STANDARD 2 - LEARNING FROM INCIDENTS, SUCCESSES AND FAILURES

Incidents, successes and failures are an opportunity to check the risk register and make adjustments to its content based on the required actions listed below. Risk owners need to ask the following questions:

- Did we identify the risk and causes?
- Why did our controls work or fail - did we identify the controls?
- Did we detect a control gap?
- Should we change our analysis?
- What further risk treatment is required now?

At this review stage where changes are detected and in accordance with the Risk Assessment Process updates are to be made to the risk register.

7.3 STANDARD 3 - RISK OWNERSHIP AND MANAGEMENT

A risk owner is defined as "A Council employee (usually a Director and/or Manager) authorised by the CEO, through this document, to manage a particular risk and is accountable for doing so."

For Corporate Risks, the CEO will delegate a Director or Manager to own and report on specified corporate risks.

For risks at a departmental and sectional level, Directors and Managers will maintain the ownership of these risks. However it is expected, according to specific need, that they will allocate the day to day management of some of these risks, particularly those with a lower current risk rating, to Coordinators or Supervisors.

For risks relating to capital projects and major events, Directors and Managers will maintain the overall ownership of these risks; unless the CEO nominates another Council employee to own the risks for a specific project or event. For risk reporting purposes, capital project and major event risks must be documented in the risk register by the risk owner.

8. RISK MANAGEMENT PROCESS

The risk management process must be an integral part of management, embedded in the culture and practices of Council, and tailored to our operational and business processes. The risk management process (shown in Figure 3 taken from AS/NZS ISO 31000:2018 - Risk Management Guideline) involves establishing the context, assessing the risk, treating the risk, monitoring the risk and reviewing the risk. The whole process needs to be communicated to stakeholders who are consulted with throughout the process. (see Figure 3 Summary of Council's Risk Management Process)

Mareeba Shire Council's **Enterprise Risk Management Process** provides the detail for Risk Assessment. This process includes the thresholds for 'likelihood' and 'consequence' as determined by Council as well as the Risk Rating Matrix which enables the Risk Rating to be determined for each identified risk.

This process also guides the user as to what action needs to be taken depending on the inherent risk as calculated. For example a risk with an Extreme Rating requires immediate action and must be reported to the CEO, while a risk that has a Low rating may not require any treatment other than ongoing monitoring.

The establishment of the context is specific to each individual risk. The key stakeholders will vary from one risk to another and should include individuals from a range of levels who are involved in the delivery of the service or identified activity.

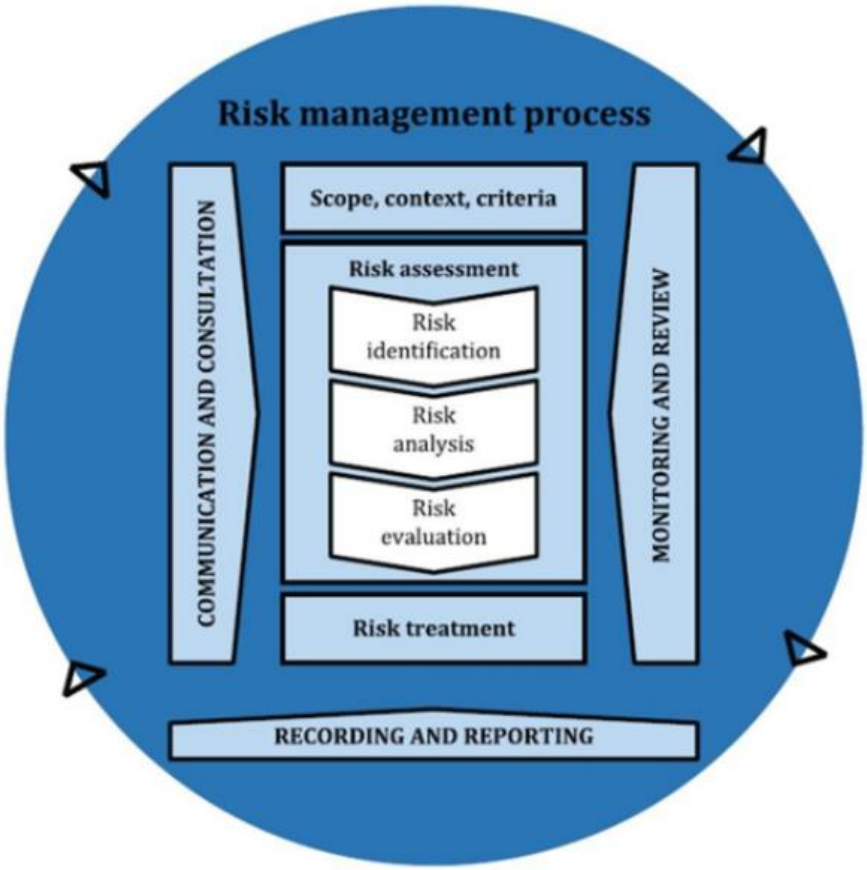

Figure 3 - Summary of Council's Risk Management Process

9. RESOURCES

Risk management needs to be appropriately resourced to maintain an effective and stable process to increase awareness, responsibility and ownership of Council's risk management principles. Resourcing considerations include:

- employees, skills, experience and competence;
- responsibilities for each step in the risk management process;
- organisational process to manage risk;
- procedures and processes;
- supporting technology system; and
- risk management training.

10. INSURANCE

Council's insurance portfolio is managed by the Governance Section. All insurance policies are to be sourced through this section and not by the individual business areas.

10.1 INSURANCE AS A RISK MANAGEMENT TOOL

Council should use its available resources efficiently and effectively to manage risk, minimising loss to the community and its assets. Insurance may be used to transfer or manage the risk of financial loss however, in some instances it may not be cost beneficial to do so and may not be transferable in every instance.

When considering the use of insurance the following should be considered:

- Nature of the risk;
- Availability of alternative risk management and mitigation strategies;
- Financial consequences of choosing not to insure; and
- Level of loss Council is willing to fund.

Responsible officers must ensure they have the appropriate insurances for their specific risks. The level of insurance required should be based on tolerance levels, past claims experience, the availability and cost of insurance. Officers should:

- Ensure they consider all insurable risks and insure appropriately; and
- Consider Council's risk profile and determine the appropriate level of insurance required.

Preventative and mitigating measures should be considered to reduce the probability or severity of an adverse risk event occurring, if proven to be of cost-benefit, even if the risk has been insured. Regardless of whether the risk is able to be insured or not, the risk owner should document how the risk is to be managed via the risk register.

11. TRAINING

The Manager Development & Governance will be responsible for ensuring adequate training is provided to employees involved in the risk management process.

12. RAISING AWARENESS OF RISK MANAGEMENT

One mechanism to raise awareness of enterprise risk management with the Senior Management is to put a greater emphasis on the following section headings in Council reports, with the risk implications being a mandatory component of the reports;

- link to Corporate Plan,
- consultation
- legal and risk implications,
- policy implications,
- financial & resource implications

Council Reports must identify risks, particularly those with Significant and Extreme risk ratings. Where such risks have been identified an action item must be created to ensure that the register is updated in a timely fashion. This is also an opportunity to discuss the status of any risk treatment implementation plans.

13. REVIEW OF ENTERPRISE RISK MANAGEMENT DOCUMENTS

Item	Process
Risk Management Policy	Document to be reviewed by Councils Senior Management Team every two years or when there is a major change in Council. To be approved by Audit Committee and Council.

Risk Management Framework	**Document to be reviewed every two years with changes to be endorsed by the Audit Committee and approved by the Council. May also be reviewed where improvements are identified.**
Risk Management Process	Document to be monitored and reviewed on an ongoing basis and changes to be endorsed by the Audit Committee and approved by the EMT.
Strategic Risks (Organisational level)	Directors and CEO to review all strategic and operational risks (significant to extreme) and treatments. Report to Audit Committee on annual basis or where a change is made.
Operational Risks (Department level)	Managers to review risks and treatments when data at the task level has changed. Regular reviews to be undertaken (on all significant risks) and reported to the EMT.
Individual risks (Task level)	The monitoring and review will be ongoing. Checking the process used reflects up to date information. May be prompted by an incident where a control failed or was not in place.