ROCKHAMPTON REGIONAL COUNCIL

ENTERPRISE RISK MANAGEMENT

FRAMEWORK

Review Timelines

This document will be reviewed when any of the following occur:

(a) The related information is amended or replaced; or

(b) Other circumstances as determined from time to time by Council.

Document Management

Sponsor	Chief Executive Officer
Business Owner	Chief Executive Officer
Policy Owner	Chief Audit Executive
Policy Quality Control	Corporate Improvement and Strategy

Version Control

Version	Change	Date
2.0	Reviewed with minor amendments including reflecting new Values and Goals; and who is responsible for documenting and reporting project/event risks	January 2018
1.1	Reviewed with minor amendments	October 2015
1.0	Original Adopted Version	25 June 2013

TABLE OF CONTENTS

1 Introduction

Acknowledgement is gratefully given to SAI Global for their permission to reproduce, and base parts of the following work on, AS/NZS ISO 31000:2009 as per SAIG REF: 1102-c134 letter and verbal permission.

As defined in *AS/NZS ISO 31000:2009 - Risk Management - Principles and Guidelines*, **risk** is the "***effect of uncertainty on objectives***". 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 activities and 'tools' to identify and mitigate the risk of uncertainty in meeting Council's strategic and operational objectives.

Enterprise risk management is more than risk management. Enterprise risk management is an integral part of Council's activities and should be integrated using 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 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 Procedure.

The implementation of this framework will:

- provide 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

Council's Mission is to create a region that our community values and others admire.

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.

The following are our values and aligned behaviours:

Accountable – We are proactive and take personal responsibility. We are clear on our expectations, if in doubt we seek clarification. We do what we say we will do and deliver our promises on time. We hold ourselves and other accountable. We take personal accountability for our own and others safety. We trust individuals to do their jobs.

Customer Focused – We are timely and responsive to our customers and community. Our decisions and actions have the customer and community at the front of mind. We engage with and listen to the customer. We support each other to achieve the best outcome for the customer.

One Team – We work together to find solutions and opportunities. We openly share knowledge, information and resources in order to deliver the best outcome for the Council. We talk with each other and seek ways to collaborate. We understand our shared goals and how each area fits together. We develop solutions with the big picture in mind ensuring we encourage collaboration and consider the impact on others. Communication and engagement are priorities at all levels.

Continuous Improvement – We take the time to explore better ways to do things. We listen to and genuinely value ideas from all staff. We accept mistakes will happen and we ensure we share the learning's. Continuous improvement is valued as an opportunity not an expense. We will be open to change, have an open mind and maintain a positive attitude.

People Development – Leaders coach, support and listen to their people. We support and develop our people to ensure they can reach their full potential. We will seek and provide feedback with the constructive intent. Development is focused on technical and behavioural capability. People are valued and treated with respect regardless of position.

1.3 Enterprise Risk Management 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 (outcomes) are derived from the following goals:

- **Community** – A connected community that values a sense of belonging; where residents celebrate their diversity and have modern services available to support a safe, healthy and engaged lifestyle now and into the future.
- **Economy** – A thriving regional capital that creates and nurtures diverse opportunities to balance work, play and growth.
- **Environment** – An environmentally balanced and aware community, which preserves and maintains our natural environment and incorporates contemporary and proven sustainability principles, as part of all activities for current and future generations.
- **Service Excellence** – A modern thinking, community outcome focused organisation that effectively balances the community's aspirations with the resources available now and into the future.
- **Local Government Leader** – Delivering a high performing and progressive organisation that leads by example.

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

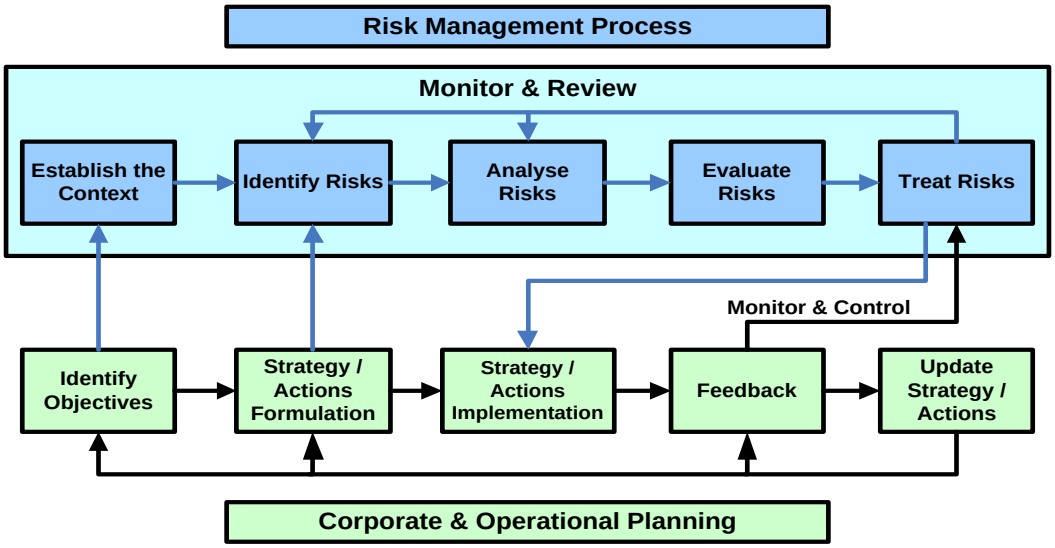


Figure 1 - Linking Corporate and Operational Planning with Risk Management

2 Purpose

The purpose of the Enterprise Risk Management Framework is to provide a consistent organisation-wide approach towards the management of risk. ERM encompasses the following:

2.1 Determining the level of risk Council is prepared to accept.

2.2 Development of proactive strategies to identify, control, treat and manage those risks.

2.3 Developing and promoting a positive risk management culture, integrated throughout Council as part of the day-to-day business and organisational activities.

2.4 Strengthening sound corporate governance practices, supporting informed decision making, priority planning, budgeting and reporting.

2.5 Improving operational effectiveness and efficiency, and communication of risk throughout the organisation.

2.6 Establishment of organisational roles, responsibilities and accountabilities for risk management.

3 Related Documents

Local Government Regulation 2012

AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines

Business Continuity Management Policy

Capital Project Management Framework Policy

Corporate Plan

Disaster Management Policy

Enterprise Risk Management Policy

Enterprise Risk Management Process Procedure

Fraud and Corruption Control Plan

Fraud and Corruption Control Policy

Fraud and Corruption Risk Checklist

Operational Plan

Workplace Health and Safety Procedure No. WHS-WP-2.3.1– Risk Management

Assorted asset management plans and risk registers

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	Rockhampton Regional 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. This process determines the level of risk and provides the basis for decisions about risk treatments.
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 general manager 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.
Wider Leadership Team	For the purpose of implementing the ERM framework this refers to the CEO, General Managers, Managers (1st, 2nd and 3rd level management) and other employees approved by the CEO to be a risk owner.

**Definitions based on ISO31000:2009*

5 Risk Management Principles

This ERM framework is based on the following risk management principles:

5.1 Adds value - Risk management is integrated with Council's Corporate and Operational Planning (and budget deliberation process), contributing to the achievement of objectives and facilitating continual performance improvement leading to good governance, operational efficiencies and improved risk management maturity.

5.2 ERM is an integral part of all organisational processes - Risk management takes into account human and cultural factors and is part of the responsibilities of management and an integral part of Council's processes, including strategic and operational planning, workplace safety and change management processes.

5.3 ERM informs all decision making - Risk management assists decision makers in making informed decisions, prioritising actions and identifying alternate courses of action as necessary.

5.4 **ERM promotes a safer work environment** - Risk management integrated with Council's Workplace Health and Safety framework and systems, promotes safe work practices and a safer work environment.

5.5 **Explicitly addresses uncertainty** - Risk management clearly takes account of uncertainty, the nature of uncertainty and how it can be addressed.

5.6 **Systematic, structured, timely and tailored** - Risk management, tailored to meet Council's corporate and operational objectives, provides a systematic, timely and structured approach to improving efficiency and contributes to consistent, comparable and reliable results.

5.7 **Based on best available information and experience** - Risk management is based on the utilisation of generally accepted risk mitigation techniques for managing risks including historical data, experience, stakeholder feedback, observations, forecasts and expert judgment.

5.8 **Transparent, inclusive and responsive to change** - Risk management provides for appropriate and timely involvement of stakeholders, particularly decision makers at all levels, and ensures that risk management remains relevant and up to date as new risks emerge, some change and others disappear.

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:

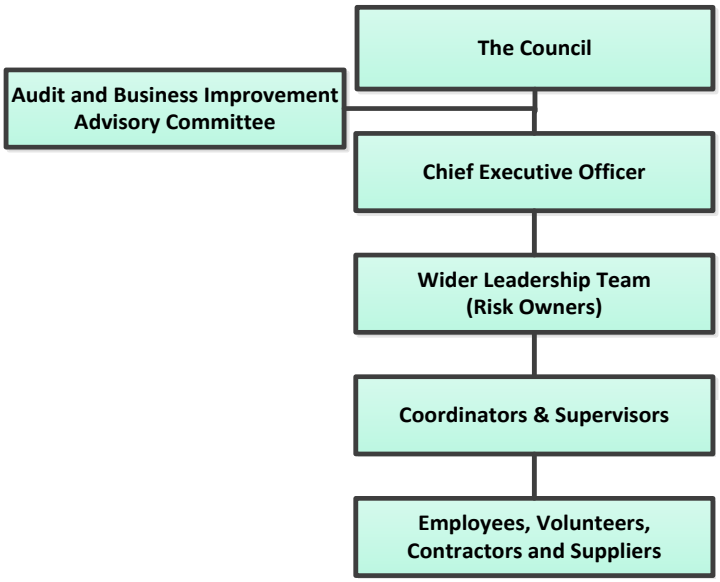


Figure 2 - ERM Governance Structure

6.1 The Council

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

6.1.1 Adoption of Council's ERM Policy, risk registers and any updates. These ordinarily will be first reviewed by Audit and Business Improvement Advisory Committee if the timing of their meetings allow for it;

6.1.2 Monitoring 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;

6.1.3 Satisfying itself that the as low as reasonably practicable (ALARP) evaluation of risks with an existing high or very high current risk rating is tolerable;

6.1.4 Satisfying itself that risks with lower ratings are effectively managed, with appropriate controls in place and effective reporting structures; and

6.1.5 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 systems for effectively managing the risks that may affect the achievement of Council's corporate and operational objectives specifically Council's ERM framework, policies and procedures.

6.3 Wider Leadership 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 Wider Leadership Team, as the **risk owners** within their areas of responsibility, are responsible for:

6.3.1 Promoting and overseeing the development of a positive risk management culture throughout Council;

6.3.2 Providing direction and guiding the inclusion of risk management in all corporate and operational decision making;

6.3.3 Possessing a clear understanding of the risk profile relating to their area;

6.3.4 Maintaining the framework for managing, monitoring and reporting risk in line with Council's corporate and operational objectives;

6.3.5 Performance against the risk register. This is an Operational Plan target and will be assessed as applicable;

6.3.6 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;

6.3.7 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, for example, the risk isn't being over or under controlled; and

6.3.8 Ensuring adequate resourcing and risk management training for 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 (for example, 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:

6.5.1 Meeting their obligations under relevant legislation (including Workplace Health and Safety) and the ERM framework;

6.5.2 Acting at all times in a manner which does not jeopardise the health and safety of themselves or any other person in the workplace;

6.5.3 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;

6.5.4 Identifying areas where risk management practices should be implemented and documented, advising their supervisors accordingly; and

6.5.5 Reducing the risk and minimising the impact of fraud and corruption within their work environment.

6.6 Audit and Business Improvement Advisory Committee

The Audit and Business Improvement Advisory Committee is an advisory committee which provides specialist high level advice and oversight with respect to matters of financial reporting, corporate governance, risk and control, compliance, and internal and external audit functions.

The Audit and Business Improvement Advisory Committee is accountable to the Council, advising of its activities, findings and recommendations including risk management matters. The Committee is to review the risk registers and/or any updates, as presented, for adoption by Council.

7 Council 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 - Supported Audit Recommendations Require Risk Conversion

Risks identified through either an internal or external audit must be placed in the appropriate risk register by the risk owner (the Senior Risk and Assurance Advisor 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?

A root cause analysis (verifying the specific underlining causes) will assist with this process.

Undertaking this process will assist in ensuring a closed loop process is in place and that the risk is being actively managed.

7.3 Standard 3 - Risk Ownership and Management

A risk owner is defined as “A Council employee (usually a General Manager 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 General Manager or Manager to own and report on specified corporate risks.

For risks at a departmental and sectional level, General Managers 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, General Managers 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 and reported in the risk register by the project/event manager.

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 at *Figure 3*) comprises of establishing the context, risk assessment, risk treatment, risk monitoring and reviewing, and stakeholder communication and consultation.

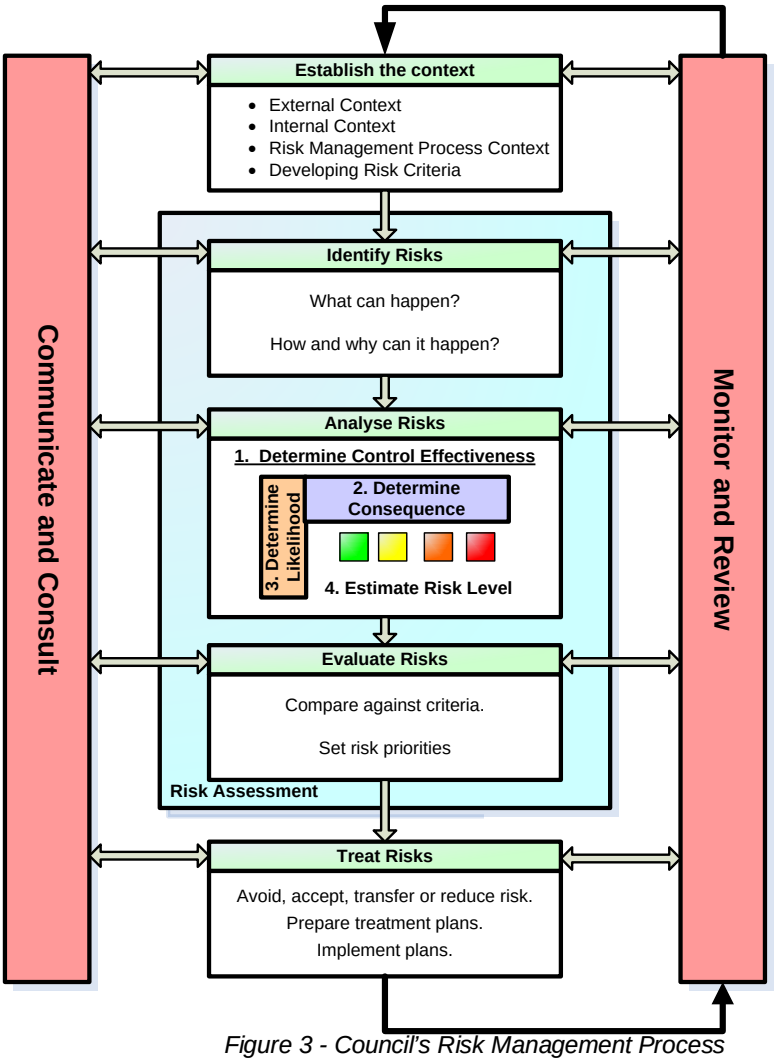


Figure 3 - Council's Risk Management Process

8.1 Communicate and Consult

Communication and consultation are integral parts of, and must occur throughout, the risk management process for all stakeholders. It is important to communicate and consult with stakeholders at each step of the risk management process. Communication efforts must be focused on consultation and two-way dialogue, rather than a one-way flow of information from decision makers to stakeholders. This provides a shared and better understanding of risks identified and the appropriate treatment options.

Communication is useful in resolving differences in perceptions and comprehending risks by understanding that different factors can contribute to the risk assessment process (for example, an expert's perspective may differ from a lay person, but the differing perspectives may also contribute to the process).

To limit ambiguity and duplication, risk assessments and treatments should be undertaken in a group environment with key stakeholders in attendance. Any uncertainties should be discussed to determine basic assumptions, measurements and mitigation strategies.

The Senior Risk and Assurance Advisor will be available to assist employees throughout the risk management process including risk assessments, developing treatments and reporting.

Any changes to the ERM framework that impacts the process is to be communicated to all stakeholders.

Please also refer to Monitor and Review (section 8.5) for the reporting regime.

8.2 Establishing the Context

As depicted in Figure 3, the first step in the risk management process is to determine the context to which the assessment process is being applied. This step provides value to the process as it is where the alignment, planning, understanding and preparation occur. The context, internal or external, refers to the environment in which Council seeks to achieve the particular objective being risk assessed. This includes:

8.2.1 External Context

- The cultural, social, political, legal, regulatory, financial, technological, economic and natural environment - international, national, state or local;
- Key drivers and trends having impact on Council's objectives; and
- Relationships with, and perceptions and values, of external stakeholders.

8.2.2 Internal Context

- Governance, organisational structure, roles and responsibilities;
- Corporate and operational plans, policies and objectives, and the strategies in place to achieve them;
- Organisational capabilities, in terms of resources, knowledge, systems and technology;
- Relationships with, and perceptions and values of, internal stakeholders; and
- Information systems and decision making processes.

The risk management context considers the goals, objectives, strategies, scope and parameters of Council activities that could be a source of uncertainty or those parts of Council where the risk management process is being applied. This includes consideration of the benefits, costs and opportunities of risk management activities and the resources required. Setting the risk criteria is also part of establishing the context.

8.3 Risk Assessment

The risk assessment is the overall process of risk identification, analysis and evaluation. The ERM Process Procedure details the risk assessment and treatment process and includes:

- The Risk Calculator, and associated Risk Consequence and Likelihood Tables; and
- Guidance on control effectiveness and treatment plans.

NB: Site specific risks relating to workplace and public safety are assessed utilising the risk calculator and associated safety consequence/likelihood descriptors. These site specific workplace and public safety risks are to be documented via Council's Safety Unit's systems.

8.3.1 Identifying the Risks

Risk identification determines what, where, when, why and how risks could arise and the effect on Council's ability to achieve its objectives. A comprehensive list of risks is generated based on **events** that may create, enhance, prevent, degrade, accelerate or delay the achievement of Council's objectives. The identification activity should also include risk associated with not pursuing an opportunity as well as any risks not under Council's control.

The method of identifying Council's risks involves a range of process and learned activities including, but not limited to:

- Brainstorming
- Team Meetings
- Knowledge
- Experience
- Benchmarking
- Industry experts
- Previous risk assessments
- Flowcharts
- SWOT analysis (Strength, Weaknesses, Opportunities and Threats)
- Checklists

A second element of the risk identification process should include determination of the possible causes of the risk and subsequent consequences, including cascade and cumulative effects. It should be noted that at this point in the process it is important to include all risks regardless of whether or not their source is under Council's control.

8.3.2 Analysing the Risks

Risk analysis is a process using predetermined criteria to assess the level of risk based on the consequences and likelihood of a risk eventuating. The risk analysis stage provides an input to risk evaluation and to decisions on whether risks need to be treated.

Risk analysis is important as the outcome of the analysis assists in determining if any further treatment (additional controls) is necessary to modify the risk.

During risk analysis, consideration must be given to the causes and sources of risk, their positive or negative consequences, the likelihood that those consequences can occur, and the effectiveness of any existing controls.

The analysis steps are:

8.3.2.1 **Identify existing controls** - the controls that are currently in place to reduce the risk must be considered. Controls can include any policy, procedure, process, mechanism, practice or other actions which modify the consequences and/or their likelihood.

8.3.2.2 **Rate the consequences** - the consequences reflect the extent of the impact on objectives. The consequences are considered in the context of the listed consequence categories and consequence examples, provided in the risk calculator and in the ERM Process Procedure, and the most likely severity or degree of each consequence. Consequence ratings from 1 to 5 are used when considering the range of impacts on Council and the community. The greater the significance of the consequences on Council and the community the higher the risk rating.

8.3.2.3 **Rate the likelihood** - likelihood is the chance of the consequence eventuating. The likelihood ratings ranging from A to E, located in the risk calculator, are used when considering the likelihood of a risk consequence eventuating.

8.3.2.4 **Determine the level of risk** - the combination of consequence and likelihood will produce a level of risk using the risk calculator. The severity ranges from low and moderate to high and very high.

N.B: All consequences and their likelihood should be rated to be able to determine which has the highest level. The highest level should then be recorded in the risk register.

Generally, risk identification and analysis tends to focus on the negative consequences of risk, and the consequence table normally reflects the negative or detrimental impacts. However, the risk management approach can be used to identify and prioritise opportunities with positive or beneficial consequences to enhance decision making and the achievement of objectives. The risk calculator has been structured to include the assessment of all risks that Council may face.

8.3.3 Evaluating the Risks

Risk evaluation is about deciding whether risks are acceptable (ALARP) or unacceptable. The purpose of risk evaluation is to assist in making decisions on the outcomes of the risk analysis; in particular which risks require further treatment and the priority for implementing those treatments.

Where risk treatment produces a business benefit, further control is necessary and a risk treatment plan will need to be developed. Generally, risks with high and very high current risk ratings will require further treatment. Risks with low and moderate current risk ratings need to be considered together with the context to determine if further treatment is necessary.

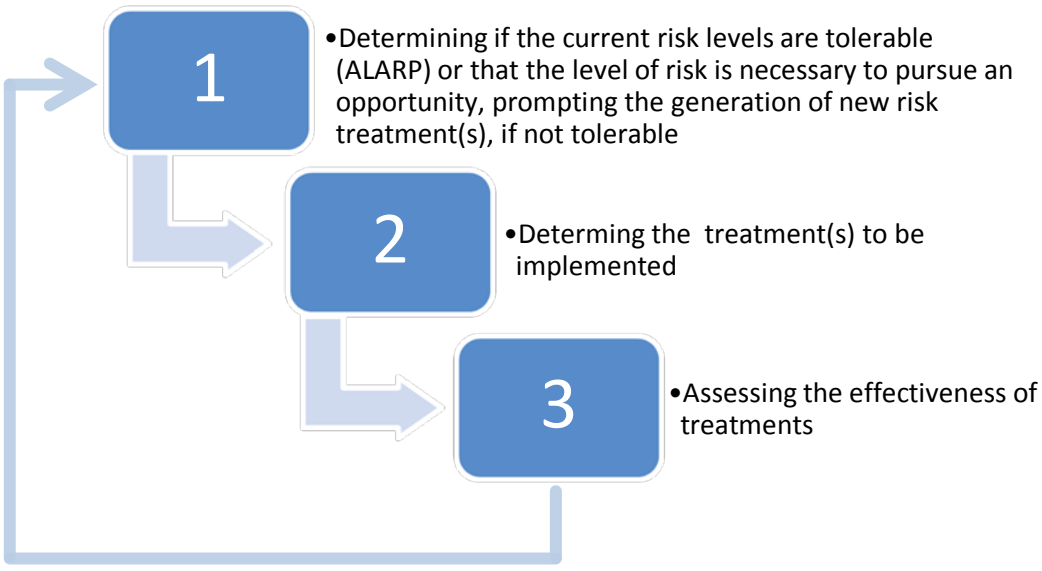
N.B.: Risks that affect other Council departments/sections/units need to be communicated to those areas and in-turn those people need to be included in the analysis and evaluation processes to ensure that risk treatments are appropriate from a whole of Council perspective.

Taking into account the decision by Council to accept a risk based on the evaluation, Council has determined that the risk is ALARP. In this case the risk owner has decided that the current risk rating is acceptable to Council. For a risk to be ALARP it must be possible for the risk owner to demonstrate that the cost involved in reducing the risk further would be grossly disproportionate to the benefit gained. The ALARP principle arises from the fact that infinite time, effort and money could be spent on the attempt of reducing a risk to zero with little or no further benefit to Council or the community.

8.4 Treat Risks

Undertaking risk treatments over and above the existing controls will be necessary for those risks determined to be unacceptable (not ALARP) or that the level of risk is necessary to pursue an opportunity. Risk treatment involves selecting one or more options for modifying risks and then implementing those options to achieve a current risk rating subsequently evaluated as acceptable.

Risk treatment is a cyclical process of:



Risk treatment options include:

- Risk avoidance and opportunity seeking (do something new or different);
- Modifying the likelihood (reduce the likelihood or opportunity susceptibility);
- Modifying the consequences (reduce the negative impacts or enhance the positive impacts);
- Risk and opportunity sharing (transform the risk or opportunity, for example, insurance, contracts, joint ventures); or
- Retaining the risk by informed decision, and monitor the controls and risk.

All of the above should be considered. Often, several in combination are more effective than just one measure.

8.5 Monitor and Review

Monitoring and review ensures that changing context and priorities are managed and emerging risk are identified. Included in this step are:

- Monitoring and review of controls (effectiveness, adequacy, changes in risk environment etc);
- Learning lessons from successes and failures in terms of root causes and control effectiveness;
- Improving the risk management process; and
- A combination of audit processes and line management review etc.

All risk assessments and treatments will be conducted in accordance with the ERM Process Procedure. All relevant documentation must be placed in Council's electronic recordkeeping system - Enterprise Content Management (ECM).

The Senior Risk and Assurance Advisor will collate all risks into the Risk Register for future monitoring and they will be communicated via the following reports:

8.5.1 Quarterly Reporting

8.5.1.1 As part of the risk monitoring and reporting régime, the Property and Insurance Unit are to report on property fraud, loss and theft to Council via the Audit and Business Improvement Advisory Committee.

8.5.1.2 The Senior Risk and Assurance Advisor is to prepare a quarterly report, from the Corporate and Operational Risk Registers, on:

- All risks with high and very high current risk ratings;
- Any risks, regardless of their risk rating, that have been identified as requiring treatment; and
- Full details of any risks previously adopted by Council or new risks, that have subsequently been amended or added since the previous reporting period.

These quarterly risk reports should be presented to Council through the Audit and Business Improvement Advisory Committee where possible. This will confirm Council's approval for the continued tolerance of those risks with a current risk rating of high and very high as well as the highest level of monitoring for those risks undergoing treatment.

8.5.2 Annual Reporting

8.5.2.1 In addition to the above, the Senior Risk and Assurance Advisor will include in the report (annually) all risks assessed as ALARP (acceptable); regardless of the current risk rating. That is: every risk will be presented at least annually.

8.5.2.2 The Fraud and Corruption Risk Checklist is to be reviewed, at least annually, and updated by the Wider Leadership Team with the results presented to Council through the Audit and Business Improvement Advisory Committee, where possible.

8.5.2.3 The results of the Qld Local Government Management Liability Scheme audit are reported by LGMS to the CEO. These are then further distributed to: Property and Insurance via the Manager Corporate and Technology Services; the Deputy CEO; and Workforce and Strategy.

8.5.3 As Needs Be Reporting

8.5.3.1 The Audit and Business Improvement Committee Policy – Terms of Reference, 3 identifies the Committee is to review reports on the activities and investigations of any significant fraud prevention and security related matters.

8.5.3.2 The Senior Risk and Assurance Advisor will develop a library of reports, including the use of graphics, to enhance the understanding of Council's successes or failures in controlling its key risks. Reports could illustrate:

- High potential exposure vs high risk rating;
- Risk rating vs control effectiveness; and/or
- Potential exposure vs control effectiveness.

8.5.4 Raising Awareness of Risk Management

One mechanism to raise awareness of risk management issues is for managers to have risk management as a standing agenda item during team meetings; particularly to highlight risks with high and very high current risk ratings. A function of this may be for employees to discuss strategies used to mitigate the risks and to build on the corporate knowledge of the team for future risk assessments. This is also an opportunity to discuss the status of any risk treatment implementation plans.

The risk registers will be reviewed and updated on a quarterly basis, or more frequently as required, by the risk owners for subsequent reporting to the Audit and Business Improvement Advisory Committee and the Council. This will be done by making proposed changes to a 'reporting' copy of the risk register. Once changes have been reviewed and agreed upon by the appropriate members of the Leadership Team, the Audit and Business Improvement Advisory Committee should review the risk registers, as presented, for adoption by Council. The Senior Risk and Assurance Advisor will then make changes to the 'control' risk register document.

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 Property and Insurance Unit. All insurance policies are to be sourced through Property and Insurance, not by the individual Council Units.

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 Chief Audit Executive will be responsible for ensuring adequate training is provided to Wider Leadership Team employees involved in the risk management process, excluding health and safety risk.

11.1 Induction Training

As part of the corporate induction training, Workforce and Strategy employees will draw reference to the ERM framework as Council's overarching risk management framework (which includes health and safety risk management). Workforce and Strategy employees will be responsible for providing adequate training in health and safety.

11.2 Risk Management Training

Employees involved in the "organisational wide" risk management process, predominantly risk owners and control owners, are to be provided risk management training by the Senior Risk and Assurance Advisor as required, excluding health and safety risk management.