ENTERPRISE RISK MANAGEMENT FRAMEWORK

Rockhampton Regional Council

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	Deputy Chief Executive Officer
Policy Owner	Chief Audit Executive
Policy Quality Control	Legal and Governance

Version Control

Version	Change	Date
2.0	Reviewed – major changes	February 2023
1.2	Reviewed with minor amendments including reflecting new Values and Goals; and who is responsible for documenting and reporting project/event risks	April 2018
1.1	Reviewed with minor amendments	October 2015
1.0	Original Adopted Version	25 June 2013

TABLE OF CONTENTS

1 Introduction

As defined in the risk management standard ISO 31000:2018, **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 (ERM) is more than risk management. It 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. Council acknowledges it also has complimentary auxiliary risk management processes, owned by and managed at the sub-element business environment level, that integrate into the ERM framework.

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

While risk is inherent in all of Council's business decisions, activities, programs, services, projects, and processes, ERM is about removing traditional divisions or barriers, including the way risk is thought about — 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 management of risk, sharing risk information across the organisation to allow effective allocation of resources and reduced duplication.

Implementation of this framework is intended to:

(a) provide a consistent and best practice approach to risk management throughout the organisation;

(b) establish a structured process for identifying, analysing, evaluating, managing, treating, monitoring, reviewing and communicating risks; and

(c) encourage the integration of proactive risk management into Council's overall governance, planning, management, reporting processes, policies, operations, values and culture.

This Enterprise Risk Management Framework should be read in conjunction with the Enterprise Risk Management Policy and the Enterprise Risk Management Process Procedure. In addition to the ERM suite of documents there are a myriad of tools and linkages in support of the framework. For example - legislation; standards; Council's values, Corporate and Operational Plans, assorted other plans and strategies, policies, procedures and guidance, and specific sub-element business environments such as workplace health and safety; disaster management and environmental sustainability, all feeding into the framework of how Council is managing risk.

2 Mandate and Commitment

Context for Council to undertake risk management is provided by several sections of legislation in the *Local Government Act 2009* and *Local Government Regulation 2012*, including the local government principles, to help facilitate effective, efficient and sustainable services while achieving Council's objectives.

While not mandated by law, there is an expectation that Council's risk management activities are undertaken within an appropriate framework. Council has selected the customisable international risk management standard, ISO 31000:2018, around which it has based its own framework and supporting processes to guide an effective ERM approach. For risk management to be effective, management is required to provide strategic and rigorous planning as well as strong and sustained commitment.

In addition to relevant legislation, best practice standards and principles, Council has an established set of values which are implicit in its work practices, including risk management, to guide the organisation in serving the community.

Council has committed to embedding risk management principles and practices into the organisation through the adoption of this framework and underlying policy as well as developing and implementing supporting procedures.

Council's Enterprise Risk Management Policy acknowledges that sub-element business environment levels of the organisation may need to have in place complimentary risk management policies and processes to meet legislative and operational needs.

For risk management to be successful everyone has a responsibility and must play their part. As an organisation we act together to achieve Council's objectives in an uncertain environment giving rise to risk. Council provides assurance that it is managing its risk through monitoring and reporting on its risks and their controls.

The following diagram (Figure 1) highlights the relationship between the high-level interrelated risk elements.

(*Figure 1*)

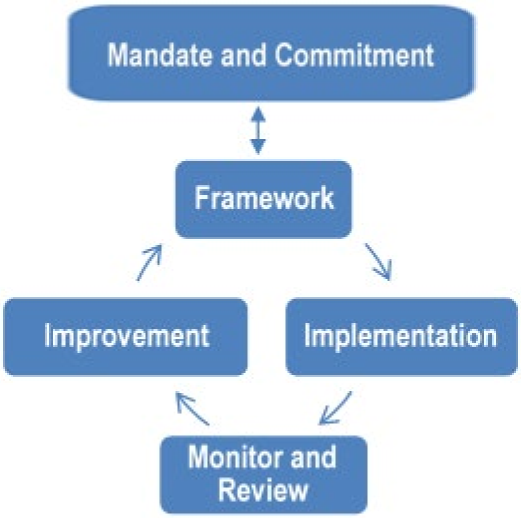
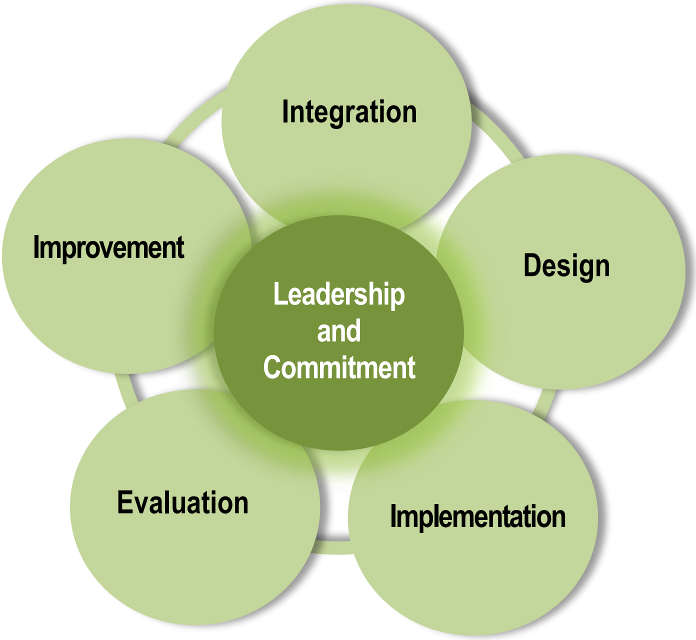


Figure 2 depicts the components of the risk management framework, as outlined in ISO 31000:2018, with leadership and commitment being central across all the components.

(*Figure 2*)



3 Purpose

The purpose of the Enterprise Risk Management Framework is to provide an overarching consistent, systematic, integrated, organisation-wide approach towards the management of risk to support the achievement of corporate goals and the budgetary process. ERM encompasses the following:

(a) Determining the level of risk Council is prepared to accept.

(b) Development of proactive strategies to identify, control, treat and manage those risks.

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

(d) Strengthening sound corporate governance practices, supporting informed decision-making, priority planning, budgeting and reporting.

(e) Improving operational effectiveness and efficiency, and communication of risk throughout the organisation.

(f) Establishment of organisational roles, responsibilities and accountabilities for risk management.

4 Related Documents

Local Government 2009

Local Government Regulation 2012

ISO 31000:2018 Risk Management - Guidelines

ISO 31073:2022 Risk Management - Vocabulary

Business Continuity Management Policy

Capital Project Management Framework Policy

Corporate Plan

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

Assorted other documents including policy documents, plans, asset management plans, and risk registers

5 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.
Contractor	A person, organisation or entity that performs a specific act or acts including the provision of services and/or materials to another person, organisation or entity under an agreement enforceable by law.
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.
Employee	Local government employee: (a) The CEO; or (b) A person holding an appointment under section 196 of the *Local Government Act 2009*.
ERM	Enterprise Risk Management 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.
ERM 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.
GM	General Manager An employee appointed to a position with a corporate band 2 delegated in line with the Delegation and Authorisation Policy and detailed in the Delegations Corporate Register, positions include Deputy Chief Executive Officer, general managers and executive managers.
Manager	An employee appointed to a position with a corporate band 3 delegated in line with the Delegation and Authorisation Policy and detailed in the Delegations Corporate Register.
Risk*	The effect of uncertainty on objectives.
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 person or entity with the accountability and authority to manage risk. Within Council this is usually a WLT employee but may include other employees authorised by the CEO to be a risk owner.
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 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/elimination/prevention/reduction.
Risk Treatment Plan	A plan detailing the process to modify risk.
Supplier	Any supplier/contractor/consultant supplying goods and/or services to Council.
Volunteer	Any person, who of their own free will, offers to undertake un-paid work for Council and is accepted as a volunteer by the CEO and/or their authorised delegates.
WLT	Wider Leadership Team For the purpose of implementing the ERM framework this refers to the CEO, GMs, and Managers (1st, 2nd and 3rd level management) and other employees approved by the CEO to be a risk owner.

**Definitions based on ISO31073:2022*

6 Risk Management Principles

This ERM framework is based on the risk management principles adopted in the Enterprise Risk Management Policy.

7 Responsibilities

The embedding 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 hierarchy of specific personnel or groups of personnel are shown in Figure 3 with their responsibilities and accountabilities described below:

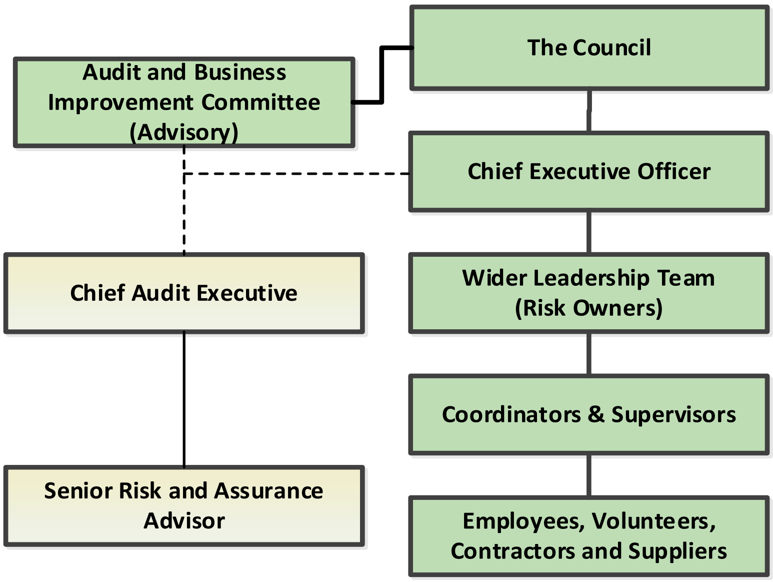

The Council
Audit and Business Improvement Committee (Advisory)
Chief Executive Officer
Chief Audit Executive
Wider Leadership Team (Risk Owners)
Coordinators & Supervisors
Senior Risk and Assurance Advisor
Employees, Volunteers, Contractors and Suppliers

Figure 3 - ERM Responsibility Structure

7.1 The Council

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

7.1.1 Where relevant, adoption of Council's policies including, Enterprise Risk Management Policy and Framework, Risk Registers and any updates. Those relating to risk management, ordinarily will be first reviewed by Audit and Business Improvement Committee if the timing of their meetings allows for it;

7.1.2 Considering risk information provided by employees to inform Council decision-making;

7.1.3 Providing adequate resources for appropriately skilled and qualified members of the Audit and Business Improvement Committee, and the financing of risk management including approved risk mitigation activities;

7.1.4 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;

7.1.5 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;

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

7.1.7 Approving major decisions affecting Council's risk profile or exposure.

7.2 Audit and Business Improvement Committee

The Audit and Business Improvement 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 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.

7.3 Chief Executive Officer (CEO)

The CEO is accountable to the Council. Under the *Local Government Act 2009* the CEO has the responsibility for managing the local government in a way that promotes the effective, efficient and economical management of public resources.

The CEO has the overall responsibility for:

7.3.1 Establishing and maintaining a risk aware culture;

7.3.2 Protecting the organisation from unacceptable costs or losses associated with Council's operations;

7.3.3 Developing, approving and implementing systems for effectively managing the risks that may affect the achievement of Council's corporate and operational objectives;

7.3.4 Supporting managers in addressing any control failures;

7.3.5 Ensuring employees receive support to fulfil their responsibilities; and

7.3.6 Delegating a GM or Manager to own and report on specified Corporate Risks.

7.4 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 WLT, as the **risk owners** within their areas of responsibility, are responsible for:

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

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

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

7.4.4 Implementing and maintaining the framework, policies and procedures, for managing, monitoring and reporting risk in line with Council's corporate and operational objectives. This includes the provision to Audit and Business Improvement Committee reports on all matters of significance received from other providers;

7.4.5 Ensuring external parties, for example, contractors, consultants etc, who are providing risk services to Council are utilising Council's adopted risk calculator/s when rating and/or describing risk, unless otherwise authorised by CEO;

7.4.6 Performance against the risk register, including updating the risk registers;

7.4.7 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;

7.4.8 Reviewing the high priority risks, at least annually, that are under-funded/under-resourced for consideration in the budget;

7.4.9 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 the risk is being adequately managed, for example, the risk isn't being over or under controlled; and

7.4.10 Ensuring adequate resourcing and risk management training for their area.

7.5 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.

7.6 All Employees, Volunteers, Contractors and Suppliers

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

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

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

7.6.3 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;

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

7.6.5 Escalating risks as per the Action Table detailed in the Risk Calculator and Tables Diagram, and

7.6.6 Minimising the risk and impact of fraud and corruption within their work environment.

7.7 Internal Audit

The role of the Chief Audit Executive (CAE) and Internal Audit, within the context of risk management, is to provide independent assessment and assurance on the adequacy and effectiveness of Council's risk management and system of internal control. The CAE has the responsibility of:

7.7.1 Supporting and providing advice to management regarding risk and internal controls;

7.7.2 Ensuring training based on ISO 31000 is available to WLT employees involved in the ERM process, excluding auxiliary risk management processes (for example, business continuity, disaster management, health and safety, etc);

7.7.3 Giving due consideration to Council's risks and risk registers in developing the Annual Audit Plan; and

7.7.4 Providing evidence-based opinions as to the adequacy of controls, within the scope of the review, when undertaking reviews from the Annual Audit Plan.

7.8 Senior Risk and Assurance Advisor

The Senior Risk and Assurance Advisor is responsible for:

7.8.1 Coordinating the enterprise risk register updates;

7.8.2 Maintaining the central copy of the ERM risk registers (Corporate Risk Register; Operational Risk Register; and Fraud and Corruption Control Risk Checklist);

7.8.3 Preparing reports for relevant parties as documented in this framework document; and

7.8.4 Providing advice, support and training as required to WLT on the ERM Framework; policy and procedures.

The officer may suggest additional risks and controls to the appropriate member of the WLT. However, the Senior Risk and Assurance Advisor is not responsible for the decision whether to implement those suggestions, nor are they responsible for the adequacy of the risks, or the internal controls, identified for a business area or function.

8 Council ERM Standards

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

8.1 Standard 1 - Supported Audit Recommendations Require Risk Conversion

Additional 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.

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

8.3 Standard 3 - Risk Ownership and Management

A risk owner is defined as “A person or entity with the accountability and authority to manage risk. Within Council this is usually a WLT employee but may include other employees authorised by the CEO to be a risk owner.”

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

For risks at a departmental and sectional level, GMs 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, through the implementation of internal controls, particularly those with a lower current risk rating, to coordinators or supervisors.

For risks relating to capital projects and major events, GMs and Managers will maintain the overall ownership of these risks unless for specific projects or events the CEO nominates another employee. However, for the purpose of reporting those risks in the ERM risk registers, they are to be documented and reported by the project/event manager for the life of the project/event, who will show as the risk owner.

9 Risk Management Process

Risk management and the internal control process is another way of viewing what Council routinely does in its day-to-day activities. That is, what they are trying to achieve has been considered, including what needs to go right, what could go wrong and what is needed to be done to make certain the right things typically happen and the wrong things are managed or avoided.

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. The risk management process (shown at *Figure 4*) comprises of establishing the context, risk assessment, risk treatment, risk monitoring and reviewing, and stakeholder communication and consultation.

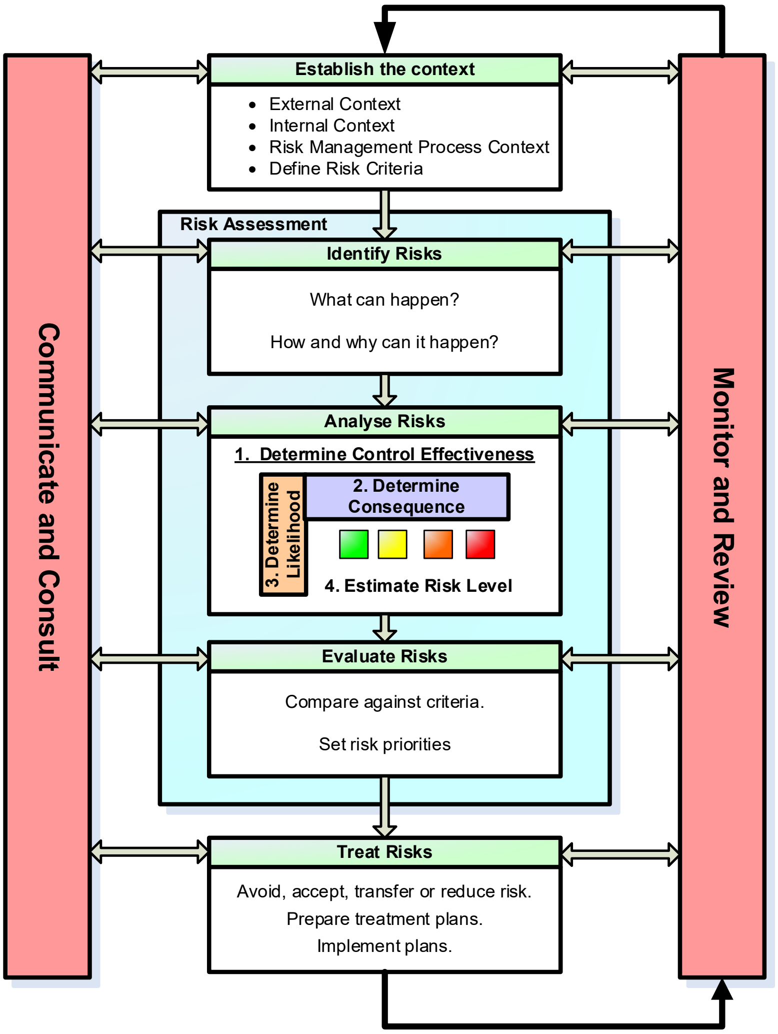


Figure 4 - Council's Risk Management Process

Council's Enterprise Risk Management Process Procedure provides detailed instructions and guidance.

9.1 Communicate and Consult

As demonstrated in Figure 4, key components that feed into making up the risk management process are communication and consultation, and monitor and review.

Communication and consultation are integral parts of, and must occur throughout, the entire risk management process. Efforts must be focused on consultation and two-way dialogue, rather than just having a one-way flow of information to facilitate risk oversight and decision-making, with the objectives being to not only assist relevant stakeholders in understanding risk but also the reasons behind how decisions were reached, and the particular actions required. The process is improved when different areas of expertise and viewpoints are brought together, resolving differences of perceptions, which can also build a sense of ownership and inclusiveness.

Awareness, of not only individual risks but managing risk, can be elevated through communication and consultation. One mechanism to achieve this is for managers to have risk management as a standing agenda item during team meetings. A function of this may be for team members to discuss strategies used to mitigate the risks and to build corporate knowledge for future risk assessments as well as to discuss the status of any risk treatment implementation plans.

Changes to the ERM Policy, Framework or Procedure are to be communicated to all stakeholders. This will usually occur through a notification in the weekly staff bulletin.

Please also *refer to Monitor and Review (section 9.2) for the reporting regime.*

9.2 Monitor and Review

For risk management to be successful in meeting the needs of the organisation, the quality and effectiveness of the design, implementation and outcomes should continually be monitored and reviewed, both the guiding documentation, and the risks themselves, to enable improvement. In this way, changing context and priorities can be managed and emerging risks identified.

All relevant documentation relating to risk management is to be placed in Council's recognised electronic recordkeeping system(s).

The Senior Risk and Assurance Advisor will maintain the central copy of the risk registers, relevant to enterprise risk management for future monitoring and the risks will be communicated via the following reports.

9.2.1 Quarterly Reporting

9.2.1.1 As part of the risk monitoring and reporting régime, the Property and Insurance Unit reports quarterly on property fraud, loss and theft to Council via the Audit and Business Improvement Committee.

9.2.1.2 The Senior Risk and Assurance Advisor is to prepare a report four times a year, 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.

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. These risk reports should be presented to Council through the Audit and Business Improvement Committee where possible.

9.2.2 Annual Reporting

9.2.2.1 In addition to the above, the Senior Risk and Assurance Advisor includes in the report all risks, regardless of the current risk rating or treatment status, annually. That is, every risk is presented at least annually.

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

9.2.2.3 The results of the Qld Local Government Management Liability Scheme audit are reported by LGMS to the CEO and are distributed as necessary throughout the organisation.

9.2.3 As Needs Be Reporting

9.2.3.1 Paragraph 4.3 of the Audit and Business Improvement Committee Policy – Terms of Reference, identifies the Committee is to (c*) receive reports on all matters of significance arising from work performed by other providers*; and (e) *ascertain that…investigations are undertaken if fraud is detected*.

These reports should be reported to the Committee by the officer who is receiving the report from the provider/s.

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.

10 Insurance

Council's insurance portfolio is managed by the Property and Insurance Unit. All insurance policies and policy amendments 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 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.

12 Training

The CAE will be responsible for ensuring ERM training, relevant to the ERM suite of documents and processes, is available to those WLT employees involved in the ERM process.

12.1 Induction Training

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

Managers are responsible for ensuring induction training for contractors and volunteers includes responsibilities under the ERM Policy and Framework.

12.2 Risk Management Training

The WLT are to be provided with ERM training, relevant to ERM suite of documents and processes, by the Senior Risk and Assurance Advisor as required. They are also required to ensure employees, volunteers, contractors and suppliers under their area of responsibility have received adequate risk management training to be able to meet their obligations.