Mount Isa City Council

ENTERPRISE RISK MANAGEMENT

“Management Framework and Guidelines”

Contents

1. Statement of Commitment

The major risk for most organisations is that they fail to achieve their strategic business or project objectives, or are perceived to have failed by their stakeholders. Mount Isa City Council is committed to establishing an environment that is not unduly risk averse, but one that enables risks to be logically and systematically identified, analysed, evaluated, treated, monitoring and managed. Risk is inherent in all of Council's activities and a formal and systematic process will be adopted to minimise and where possible eliminate all risks that directly or indirectly impact on the Council's ability to achieve the vision and strategic objectives outlined in the Corporate Plan.

This Enterprise Risk Management Guidelines have been developed to demonstrate the Council's commitment, by detailing the integrated Risk Management framework to be employed by all staff members, contractors, committees and volunteers engaged in Council business and defining the responsibilities of individuals and committees involved in managing risk.

In addition the guidelines have been developed to:

- Ensure risk management is an integral part of strategic planning, management and day to day activities of the organisation;
- Promote a robust risk management culture within the Council;
- Enable threats and opportunities that face the organisation to be identified and appropriately managed;
- Facilitate continual improvement and enhancement of Council's processes and systems;
- Improve planning processes by enabling the key focus of the organisation to remain on core business and service delivery;
- Ongoing promotion and awareness of the risk management throughout Council.

2. Introduction

In order for Council to deliver the strategies and achieve the objectives as outlined in the Corporate Plan, Council needs to identify and manage risks. Risk is an event or action, which has the potential to prevent Mount Isa City Council from achieving its corporate objectives. A risk can also be defined as an opportunity that is not being maximised by the Council to meet its objectives.

Enterprise Risk Management (ERM) is the management of risk not only in conventional hazard categories such as health and safety, IT, finance, but in the full spectrum of strategic and operational risk. ERM is the structured approach of aligning strategy, processes, people, technology and knowledge with the purpose of evaluating and managing risk. *Enterprise wide* means the removal of traditional functional, divisional, departmental or cultural barriers. Importantly by having a structured approach provides guidance to managing existing and perceived risks that have potential to impact on the organisation's commitment to fulfil its business objectives.

Effective risk management is governed by an organisation's commitment to risk management and this process is outlined in Mount Isa City Council's Risk Management Framework and Guidelines which is in line with the Australian and New Zealand Standards AS/NZS ISO 31000:2009.

3. Definitions

Risk: A risk to the business is any action or event that has the potential to impact on the achievement of our business objectives.

Risk also arises as much from the possibility that opportunities will not be realised as it does from the possibility that threats will materialise or that errors will be made.

Risk Management: Risk management for Council refers to the culture, processes and structures developed to effectively manage potential opportunities and adverse effects for any activity, function or process undertaken by the Council. Managing risk is achieved through the systematic application of policies, procedures and practices to identify, analyse, evaluate, treat, monitor and communicate risk.

Enterprise Risk Management (ERM): Enterprise risk management encompasses all the major risk categories (including financial, environmental, health and safety, fraud, information technology, compliance, security and business continuity) and includes the coordination, integration, consolidation and consistency of reporting by the various Council functions with identified risks.

Risk Register: A list of identified and assessed risks directly related to either a particular directorate or to the whole of Council. Risk Registers can either be Corporate, Operational or other project risk register.

Likelihood: The word likelihood is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively (probability or frequency).

Consequence: The outcome of an event affecting objectives (impact). An event can lead to a range of consequences. A consequence can be certain or uncertain and can have a positive or negative effect on objectives. Consequences can be expressed qualitatively or quantitatively.

Risk Owner: The person with the accountability and authority to manage a risk.

Risk Treatment: The process to modify existing risks or create new risks.

Risk Treatment Action Plans: The document that outlines the steps to be taken to reduce unacceptable risks to achievable and acceptable levels. This includes details on current controls; required risk treatments; improvement opportunities; resources; timing; reporting and accountabilities.

4. Risk Management Principles

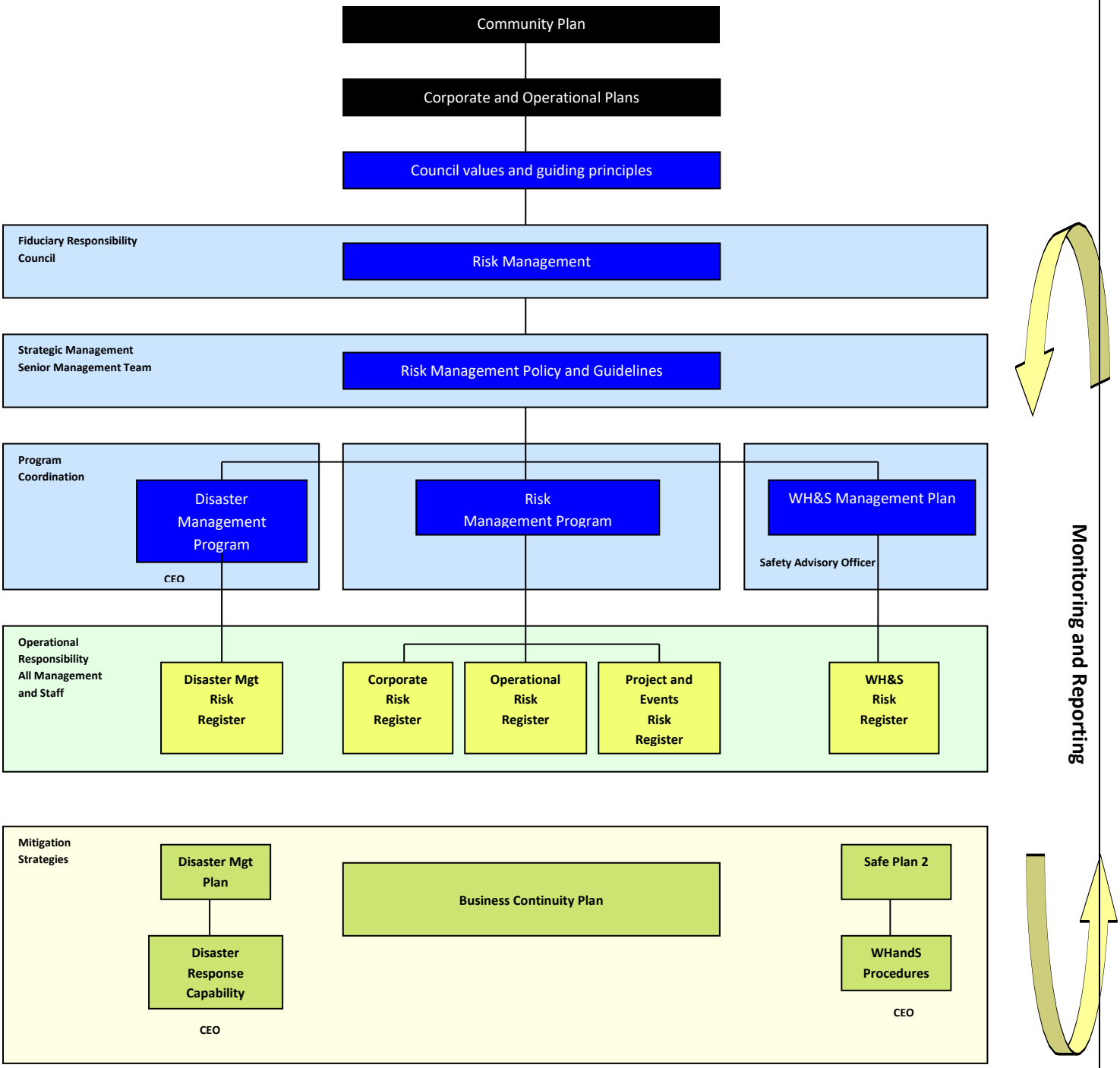
For risk management to be effective, an organisation should comply with the following principles.

Risk Management should:

- Creates and protects value;
- Be an integral part of organisational processes;
- Be part of decision making;
- Explicitly addresses uncertainty;
- Be systematic, structured and timely;
- Be based on the best available information;
- Be tailored;
- Take human and cultural factors into account;
- Be transparent and inclusive;
- Be dynamic, iterative and responsive to change;
- Facilitate continual improvement and enhancement of the organisation.

5. Risk Management Framework

The Risk Management Framework explains the relationship between the Council's risk management components and other management systems and frameworks.



6. Basis, Roles and Responsibilities

Please refer to Council's Risk Management Policy (Appendix A).

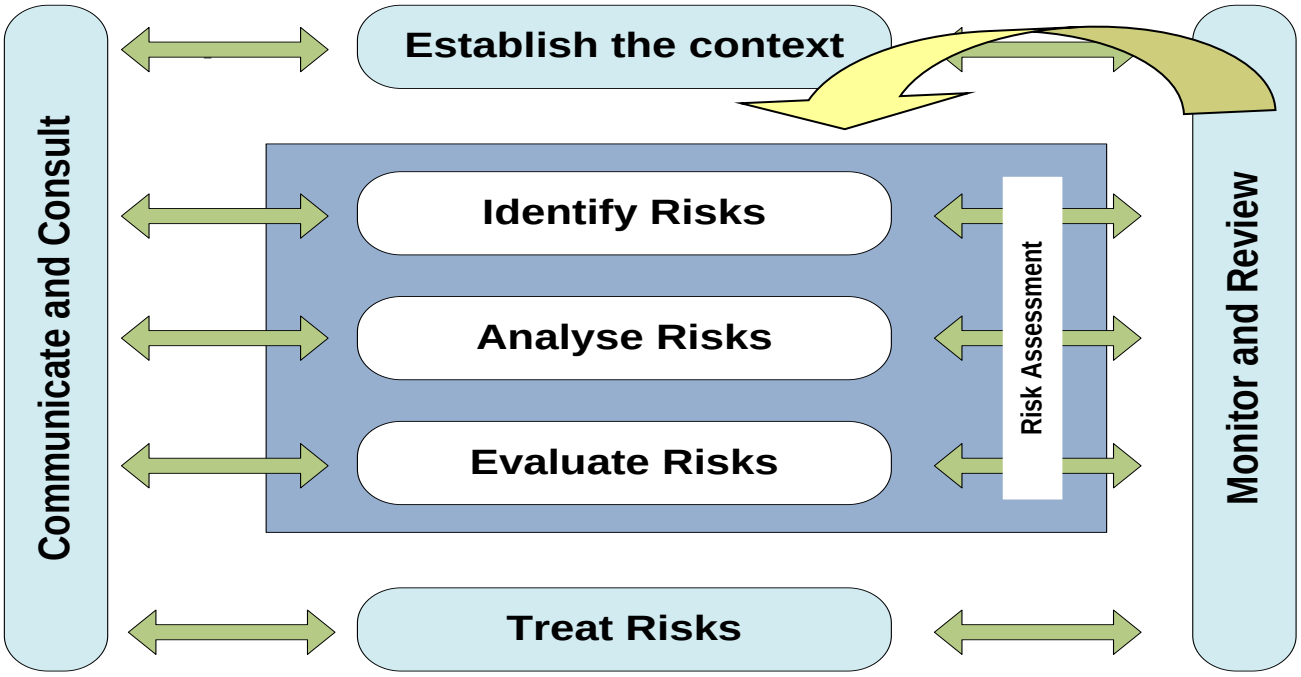
7. Risk Management Process

The process adopted by Mount Isa City Council to manage risks is in accordance with *AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines*. This process is the application of the structured risk management methodology to be used to assess; prioritise; treat and monitor risks identified. The risk management process may capture inherent risk (prior to taking into account controls in place), residual risk (after taking into account controls in place), or both.

The main elements of an effective Risk Management approach are as follows:

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

The following diagram represents the components of the Risk Management process. Each of these components is explained further below.



Source: Australian/New Zealand Standard for Risk Management – AS/NZS ISO 31000:2009

7.1 Communicate and Consult

It is an essential part of the risk management process to develop and implement an effective framework to communicate and consult with all relevant stakeholders, internal and external as appropriate, at each stage of the risk management process and concerning the process as a whole. The level of communication and consultation will vary depending on the level of interest and or influence of that particular stakeholder individual or group.

7.2 Establish the Context

Stage one of the processes establishes the strategic, organisational and risk management context in which the rest of the process will take place. This includes the criteria against which risk will be evaluated, the risk appetite of the organisation and corrective actions for the different rating achieved in the assessment of the risks.

In establishing the context for the Risk Management Framework, existing risk management processes were reviewed, interviews and workshops were held with key personnel and a Risk Management Policy was developed. (Refer to Appendix A for Risk Management Policy).

7.3 Risk Assessment

7.3.1 Identify Risks

At this stage, the organisation identifies what, why and how things can arise, that may affect the organisation, as the basis for further analysis. This is done at both strategic and operational levels of the organisation.

Categories of risk for the organisation at a strategic and operational level may include, but are not limited to:

- **Safety** – injuries, lost time, LGW and LGM claims, fatalities
- **Reputation and image** – negative media exposure, staff morale, community perception
- **Assets** – damage or loss of information, property or assets
- **Environment** – impact or harm to natural environment, potential for future damages claims and EPA prosecution
- **Service Delivery** – ability to service community and meet customer expectations
- **Regulatory** – breaches of legislation (“ignorance is no excuse”)
- **Management effort** – senior management effort directed away from achieving strategic objectives and impacting on overall performance(i.e. focused on day to day tasks)

7.3.2 Analyse Risks

This stage determines the inherent risks and then calculates any residual risks taking in to consideration any existing controls in place (existing processes and procedures). Risks are analysed in terms of consequence and likelihood in the context of those controls. The analysis will consider the range of potential risk exposure consequences and how likely those consequences are to occur. The Consequence and Likelihood are then combined to produce an estimated level of risk known as the Overall Risk Rating.

Determining Likelihood

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

Likelihood Table

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

Determining Consequence

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

Consequence Table

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

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

Consequence Matrix

Consequence	Rating	Operational – Business Continuity	Environmental	Information Technology	Strategic/Corporate Governance – Reputation - Political	Human Resources	Infrastructure, Asset and Property	Workplace Health and Safety	Financial and Economic
Catastrophic	**5**	The continuing failure of Council to deliver essential services The removal of key revenue generation	Widespread and irreversible environmental damage attributed by the courts to be negligent or incompetent actions of Mount Isa City Council.	Widespread, long term loss of IT network/hardware.	Loss of State Government support with scathing criticism and removal of the council. National media exposure Loss of power and influence restricting decision making and capabilities	Staff issues cause continuing failure to deliver essential services	Widespread, long term loss of substantial key assets and infrastructure.	Fatality or significant irreversible disability.	Above 6% of Council's annual revenue (excluding capital revenue) = $ 1M
Major	**4**	Widespread failure to deliver several major strategic objectives and service plans. Long-term failure of Council causing lengthy service interruption	Severe environmental impact requiring significant remedial action. Penalties and/or direction or compliance order incurred.	Widespread, short to medium term loss of IT network/hardware	State media and public concern/ exposure with adverse attention and long-term loss of support from the community. Adverse impact and intervention by State Government	Staff issues cause widespread failure to deliver several major strategic objectives and long term failure of day to day service delivery.	Widespread, short to medium term loss of key assets and infrastructure.	Extensive injuries. Lost time of more than 4 working days.	Between 2- 6% of Council's annual revenue (excluding capital revenue) =$500,000
Moderate	**3**	Failure to deliver minor strategic objectives and service plans. Temporary and recoverable failure of Council causing intermittent service interruption for a week.	Moderate impact on the environment; no long term or irreversible damage. May incur cautionary notice or infringement notice	Short to medium term loss of key IT network/hardware	Significant state wide concern/ exposure and short to mid-term loss of support from the community. Adverse impact and intervention by another local government and LGAQ.	Staff issues cause failure to deliver minor strategic objectives and temporary and recoverable failure of day to day service delivery.	Short to medium term loss of key assets and infrastructure	Medical treatment. Lost time of up to 4 working days.	Between 1- 2% of Council's annual revenue (excluding capital revenue) =$250,000
Minor	**2**	Temporary and recoverable failure of council causing intermittent service interruption for several days.	Minor environmental damage such as remote temporary pollution.	Minor loss/damage. Repairs required	Minor local community concern manageable through good public relations. Adverse impact by another local government.	Staff issues cause several days interruption of day to day service delivery	Minor loss/damage. Repairs required	First aid treatment. No lost time.	Between 0.2 - 1% of Council's annual revenue (excluding capital revenue) =$100,000
Insignificant	**1**	Negligible impact of Council, brief service interruption for several hours to a day.	Brief, non-hazardous, transient pollution or damage.	Damage where repairs are required however equipment still operational	Transient matter, e.g. Customer complaint, resolved in day-to-day management. Negligible impact from another local government.	Staff issues cause negligible impact of day to day service delivery	Damage where repairs are required however facility or infrastructure is still operational	No injury.	Less than 0.2 % of Council's annual revenue (excluding capital revenue) =$5,000

Determining the Overall Risk Rating

After the **consequence** and **likelihood** ratings have been determined they are combined in a matrix to determine the overall risk rating for each risk. The extent of the consequences and the extent of the likelihood risks will be assessed in a range from **Low** to **Extreme**.

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

Risk Assessment Matrix

Likelihood	Rating	Consequence				
		1	2	3	4	5
		Insignificant	Minor	Moderate	Major	Catastrophic
Almost certain	5	M	H	H	E	E
Likely	4	L	M	H	H	E
Possible	3	L	M	M	H	E
Unlikely	2	L	L	M	H	H
Rare	1	L	L	L	M	H

7.3.3 Evaluate Risks

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

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

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

7.3.4 Risk Register

A Risk Register is developed to record and assess each risk identified as part of the risk identification stage.

The application of the stages of the risk assessment process noted above ensure there is consistency in the determination of the current risk severity level, taking into account the existing controls and their level of effectiveness in mitigating or addressing the risk. Refer to Appendix B for a Risk Register Template.

Risk Profile Diagram

At the completion of the assessment process, a risk profile diagram will be developed to highlight each of the risks identified and their overall risk rating.

The risk profile diagram (example below) will highlight to CEO and senior executive the key risk exposures within the organisation. The risks will be categorised as **Extreme, High, Medium and Low** to assist management to target those risks that have the greatest potential impact on the organisation.

	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	0	0	1	1	0
Likely	0	0	1	2	0
Possible	0	3	1	0	1
Unlikely	2	6	14	0	2
Rare	0	3	0	0	0

7.4 Treatment of Risks

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

- **Retain the risk** – where the risk cannot be avoided, reduced or transferred. In such cases, usually the likelihood and consequence are low. These risks should be monitored and determined how losses, if they occur, will be funded.
- **Transfer the risk** – involves shifting all or part of the responsibility to another party who is best able to control it (such as an insurer who bears the consequence of losses eg. Insure Council vehicles).
- **Avoid the risk** – Decide not to proceed with the policy, program or activity or choose an alternative means of action.
- **Control the risk** – By either reducing the likelihood of occurrence or the consequences eg. Implement procedures for specified tasks.

Determine the most effective treatment options by considering the:

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

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

The decision to accept a risk will be determined by the agreed table indicating proposed corrective action and the risk appetite criteria established by the council. For example a LOW risk is accepted and only requires monitoring should circumstances change. For other risks, a specific management

plan may be required to be developed and implemented which may include consideration of funding. Risk treatment strategies need also be considered to ensure that no new risks are introduced.

The approach for treatment of risks is:

E	**Extreme risk** – Immediate action required. Task is not to be undertaken until detailed research and planning is completed and decision making in consultation with Strategic Management Team.
H	**High risk** – Senior management attention and action required.
M	**Medium risk** – Management responsibility must be specified and action required as soon as possible.
L	**Low risk** – Manage by routine procedures and unlikely to require additional resource.

7.5 Monitor and Review

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

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

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

- ***Monitoring*** – assess whether current risk management objectives are being achieved. Council can use inspections, incident reports, self-assessments and audits to monitor its risk management plan.
- ***Review*** – assess whether the current risk management plan still matches Mount Isa City Council's risk profile. The risk management plan may be reviewed by studying incident patterns, legislative changes and organisational activities.

Possible methods for review:

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

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

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

Recording the Risk Management Process

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

8. Reviewing the Risk Management Framework and Guidelines

In order to ensure that the risk management process is effective and continues to support the organisation's performance, all aspects of the risk management process will be periodically reviewed. The Risk Management Framework and Guidelines, Risk Management Policy and Risk Registers will be reviewed to ensure that they are still appropriate and continue to reflect the organisation's risk activities and tolerances.

Based on the results of monitoring and reviews, decisions will be made on how the Risk Management Framework can be improved. These improvements should lead to improvements in the management of risk and its risk management culture.

Review date: by 30 June 2018