Risk Management Framework

Midway Limited

ABN 44 005 616 044

(the Company)

Adopted by the Board on 22 June 2020

1. Purpose and application of this policy and framework

1.1 This policy applies to all representatives of MWY and includes staff, employees and contractors undertaking works for or on behalf of Midway Limited (MW), Midway Plantations (MWP), Plantation Management Partners (PMP), Midway logistics (MWL), Midway Tasmania (MWT), South West Fibre (SWF) and Queensland Commodity Exports (QCE), collectively known as MWG.

1.2 Midway operates in an environment where its operations and decisions must meet high standards in terms of quality and rigor. This policy recognises the importance of embedding risk management principles into our operations to successfully deliver on our objectives in accordance with our Corporate Plan.

1.3 This policy forms the framework for risk management across the organsation, the risk management procedure provides further guidance for dealing with operational risks.

1.4 The effective implementation and maintenance of the enterprise risk management framework will enable:

(a) identification of opportunities and challenges to increase the likelihood of achieving the Group's Corporate Plan

(b) Identification of a **risk appetite** to aid strategic planning and service delivery

(c) rigorous planning to support more effective decision making through better understanding of risk exposures

(d) creating an environment that enables the Group to deliver timely services and meet performance objectives in an efficient and cost-effective manner

(e) clear understanding by staff of their roles, responsibilities, and delegated authorities for managing risk to encourage a culture of accountability at all levels of the Group

1.5 Risk management is particularly important for the Group as the effect of risk realisation may have broader consequences for our stakeholders and the community.

1.6 This policy and framework applies to all staff and undertakings.

2. Definitions

2.1. Definitions are set out in the Dictionary in section 12. Defined terms are indicated in bold the first time they appear in this document.

3. Overview of the risk management approach

3.1. The Group adopts a systematic approach to risk management that identifies risks during planning of strategic, operational and project delivery. As new risks emerge they are incorporated into **risk registers**.

3.2 Strategic risks, if they occur, impact on the Group's ability to achieve the Corporate Plan or objectives.

3.3 Operational risks, if they occur, impact the Group's day-to-day service delivery and operation of it's regulatory, corporate or finance functions. These operational functions may include:

(a) Processing of Woodfibre

(b) Land management and silviculture

(c) Harvesting and Logistics

(d) Financial

(e) Information Security

(f) Work health & safety

(g) Business continuity

3.4 Project risks, if they occur, impact on the efficient and effective delivery of an individual project. Project risks may include consideration of operational risks within the scope and context of the individual project.

3.5 Each identified risk is assessed for **likelihood** and the most likely **consequence** of the risk occurring. All risks are then assigned a risk rating in accordance with the Group's **risk matrix.**

3.6 Risks are treated in accordance to the severity of their risk rating and the **risk tolerance** of the Group. It is not possible to completely eliminate all risks, therefore, a **target risk** rating is also applied to bring risks to within the Group's tolerance. Risk treatments seek to bring the current risk rating to the target risk rating by:

(a) Elimination of the risk,

(b) Isolating or removing the source of risk,

(c) Reducing the likelihood of the risk occurring,

(d) Reducing the consequence of the risk if it occurs,

(e) Sharing the risk with other parties, and/or

(f) Retaining the risk by informed decision.

4. Risk identification and reporting

4.1 **Risk reporting** is important to provide information on the monitoring of risk against the Group's objectives. A risk reporting framework allows risks to be escalated proactively when they are identified, if they exceed risk tolerance levels, or if consequences are realised.

4.2 Risks are captured on strategic, operational or project risk registers during business planning. **Developing** the risk registers is an integral part of risk management as it:

(a) Acknowledges risk as part of the decision-making process,

(b) Provides a systematic approach to defining risks and the consequences of the risks occurring,

(c) Identifies who is affected by the risk, what treatments are in place, and what actions need to be taken to control the risk, and

(d) Assigns responsibility and accountability for the management of each risk.

4.3 Risk reporting is required to inform internal and external stakeholders of the Group's risk profile, including monitoring the performance of risk treatments in order to report any change to existing risk exposures.

4.4 When risk events occur, including near misses, these risks are investigated to analyse causation and the performance of existing risk treatments. This information forms part of the ongoing reporting of risks and treatments.

4.5 The Group's internal stakeholders include:

(a) Senior Management Team,

(b) Managers,

(c) Project managers, and

(d) Staff.

4.6 The Group's external stakeholders include:

(a) The Audit and Risk Management Committee,

(b) Regulators,

(c) Members of the public including trade associations or unions, and

(d) Suppliers and contractors.

4.7 Risk information should be communicated to these stakeholders by the risk owner, using a range of formal and informal channels.

4.8 Where appropriate informal communication or risk information can include newsletters, intranet pages, emails, or notices on staff noticeboards.

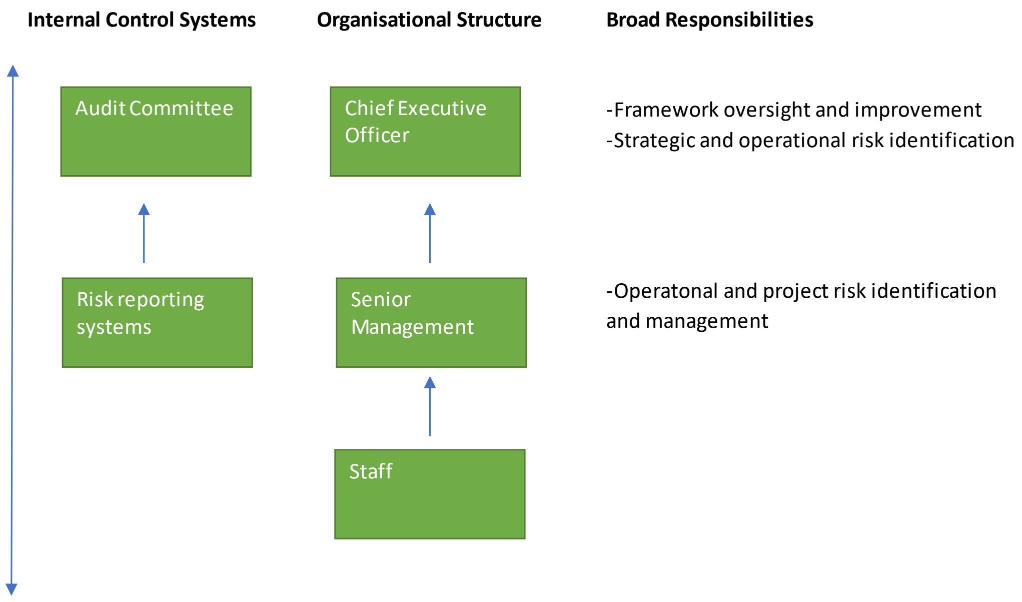


Figure 1. Risk governance, organisational structure, and support relationship.

5. Internal risk culture

5.1 The Group has a commitment to promoting a positive risk culture. Attributes of a positive risk culture include:

(a) Understanding of the nature of risk and how it affects our work and achieving our objectives

(b) Incorporating risk awareness into training for all staff

(c) Encouraging the identification, communication and reporting of risks from all levels

(d) Modelling leadership behaviours that are risk aware and making decisions that are risk-informed

(e) Incorporating risk into position descriptions and performance development plans

6. Embedding risk management into existing business processes

6.1 Risk management is of greatest benefit when aligned and integrated with other business processes. The Group's enterprise risk management framework supports the achievement of the Corporate Plan by linking directly to its objectives.

6.2 Risk is incorporated as standing items on meeting agendas for corporate planning, branch planning, project planning and team planning.

6.3 Risk awareness training is a mandatory part of staff induction training.

6.4 Risk responsibilities are incorporated into position descriptions and performance development plans for all staff.

6.5 Risk events are investigated and communicated to stakeholders.

6.6 Monitoring of risk treatments is incorporated into business intelligence functions.

6.7 Business processes are regularly tested, audited, and reviewed to ensure their efficacy.

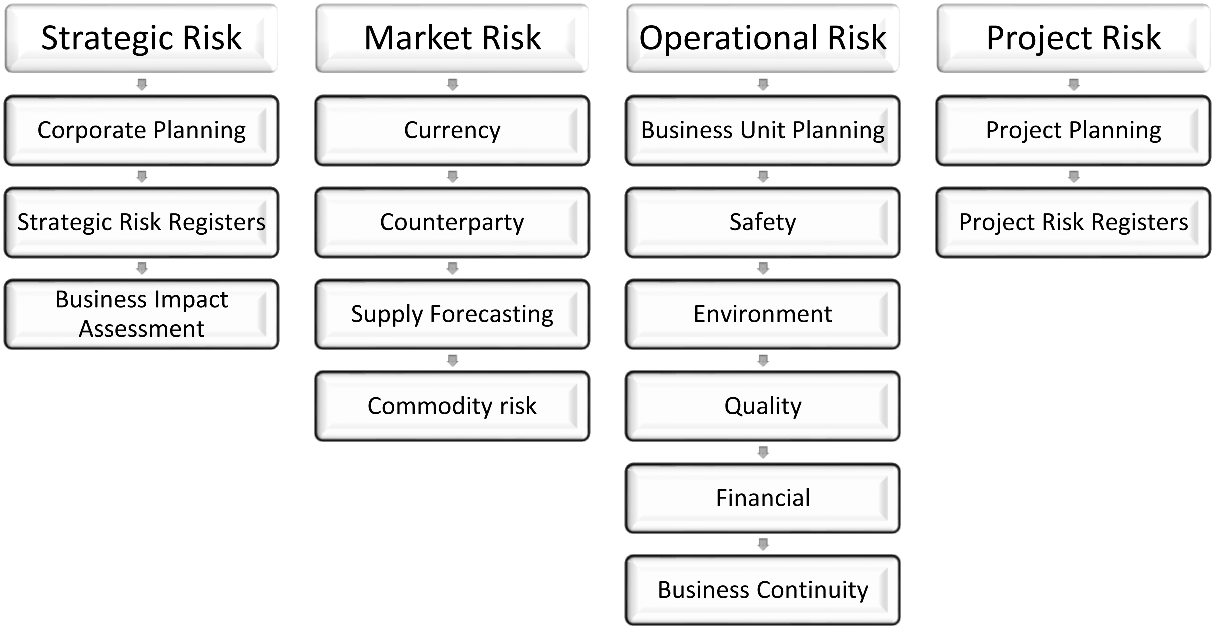


Figure 2. Organisation of risk management

6.8 Reporting cycle

Operational Risk

- Risk registers maintained by Technical Services Team (Management System database). Expanded for management of business risks.
- Business risks and financial risks identified during business planning to be uploaded and managed by each site (technical services assistance)
- Formal risk catchups to run through register to be conducted every three months (in line with ARMC)

Strategic Risk

- Strategic risks identified during business planning process to be agreed
- Strategic risk register to be coordinated and presented to ARMC every meeting
- Strategic risks to be assigned to a risk owner responsible for updating register and coordinating with relevant GM's on management of the risk

Market Risk

- Tracked and reported seperately, along with the Strategic Risk Register to the ARMC

Project Risk

- Each project to have its own formal risk assessment before being formally put to the Board

7. Key accountabilities and responsibilities

7.1 Managing Director

(a) Receiving a regularly reviewed framework

(b) Approving the framework, including the risk appetite and risk tolerance for the risk management policy.

(c) Ensuring the consistent application of the framework across the Group's functions and locations.

7.2 Audit and Risk Management Committee

The Committee's risk management responsibilities include:

(a) reviewing whether management has in place a current and comprehensive risk management framework, and associated procedures for effective identification and management of risks,

(b) reviewing whether a sound and effective approach has been followed in developing strategic risk management plans for major projects or undertakings;

(c) review the impact of the Group’s risk management framework on its control environment and insurance arrangements; and

(d) review whether a sound and effective approach has been followed in establishing business continuity planning arrangements, including whether disaster recovery plans have been tested periodically.

7.3 Senior Management Team

Leads the continuous maturity of the Group’s risk management culture across the Group and within their Division including:

(a) Reviews and endorses risk registers, and risk action plans;

(b) Identifies within the business planning process new risks to be monitored;

(c) Communicates the importance of risk management and actively supports the risk management process within their Branch.

7.4 Business Unit Managers

All Business Unit Managers are responsible for ensuring that:

(a) They continually evaluate risks and implement **Risk Treatment Plans** in relation to those risks

(b) the activities within their Business Unit are appropriately controlled

(c) a culture of risk awareness and transparency is developed within their teams

(d) they manage the risk they have accountability for

(e) they review the risk on a regular basis

(f) they identify where current control deficiencies may exist

(g) they update and report information pertaining to the risk

(h) they work with other Business Unit Managers or teams on shared risks, controls, or treatments

(i) they proactively escalate or deescalate the risk to their General Manager where the risk is increasing or decreasing in likelihood and/or consequence

(j) they provide information about the risk when it is requested, or the risk is changing in likelihood and/or consequence.

7.5 Staff (including contractors)

It is the responsibility of all staff to take account of the framework in their respective roles.

Staff focus should be upon identifying risks and reporting these to their relevant manager or supervisor. Where possible and appropriate, they should also manage these risks in consultation with their manager.

8. Risk management process

8.1 The risk owner will undertake risk management in accordance with the process adopted by the Group, outlined in Figure 3, below:

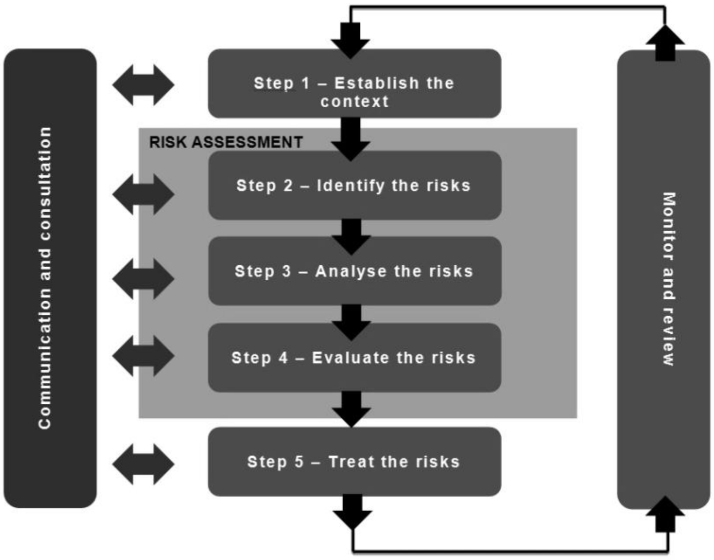

Step 1 – Establish the context
RISK ASSESSMENT
Step 2 – Identify the risks
Step 3 – Analyse the risks
Step 4 – Evaluate the risks
Step 5 – Treat the risks
Communication and consultation
Monitor and review

Figure 3. Risk management process

Communication and consultation

8.2 Communication and consultation are an ongoing and iterative process undertaken to provide, share or obtain information on known risks and treatments. Consultation:

(a) helps establish the risk context,

(b) ensures stakeholder interests are understood and considered,

(c) helps identify risks and treatments,

(d) provides a range of expertise to address risks, and

(e) secures the support and endorsement of treatment or action plans by stakeholders.

Establish the context

8.3 Context is defined by the Group as being **strategic**, **operational** or **project** level. The appropriate risk register is then selected based on the context.

Identify risks

8.4 Risks can be identified as the *effect* of an event on the organisation or project. Risk statements should focus on the effect rather than the event (For example, a fraud risk might be loss of funds while the event is inappropriate use of credit cards). Focusing on the effect keeps risks and controls at a consistent contextual level. These risks are entered into the risk register.

Analyse the risks

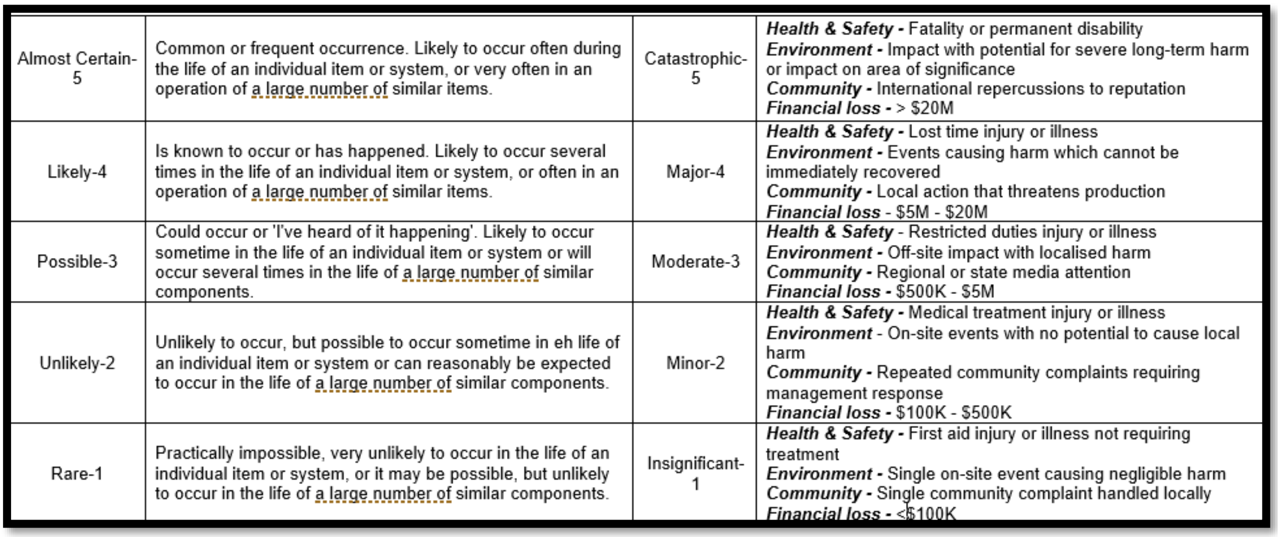
8.5 A description of the event(s) that may cause the risk to occur are added to the following column of the risk register.

8.6 The possible sources for these events are then added to the risk register.

8.7 What is captured in this first stage of **risk assessment** is the untreated risk.

Evaluate the risks

8.8 The likelihood rating can be established by considering the likelihood and consequence of it occurring using the definitions in Table 1, below:

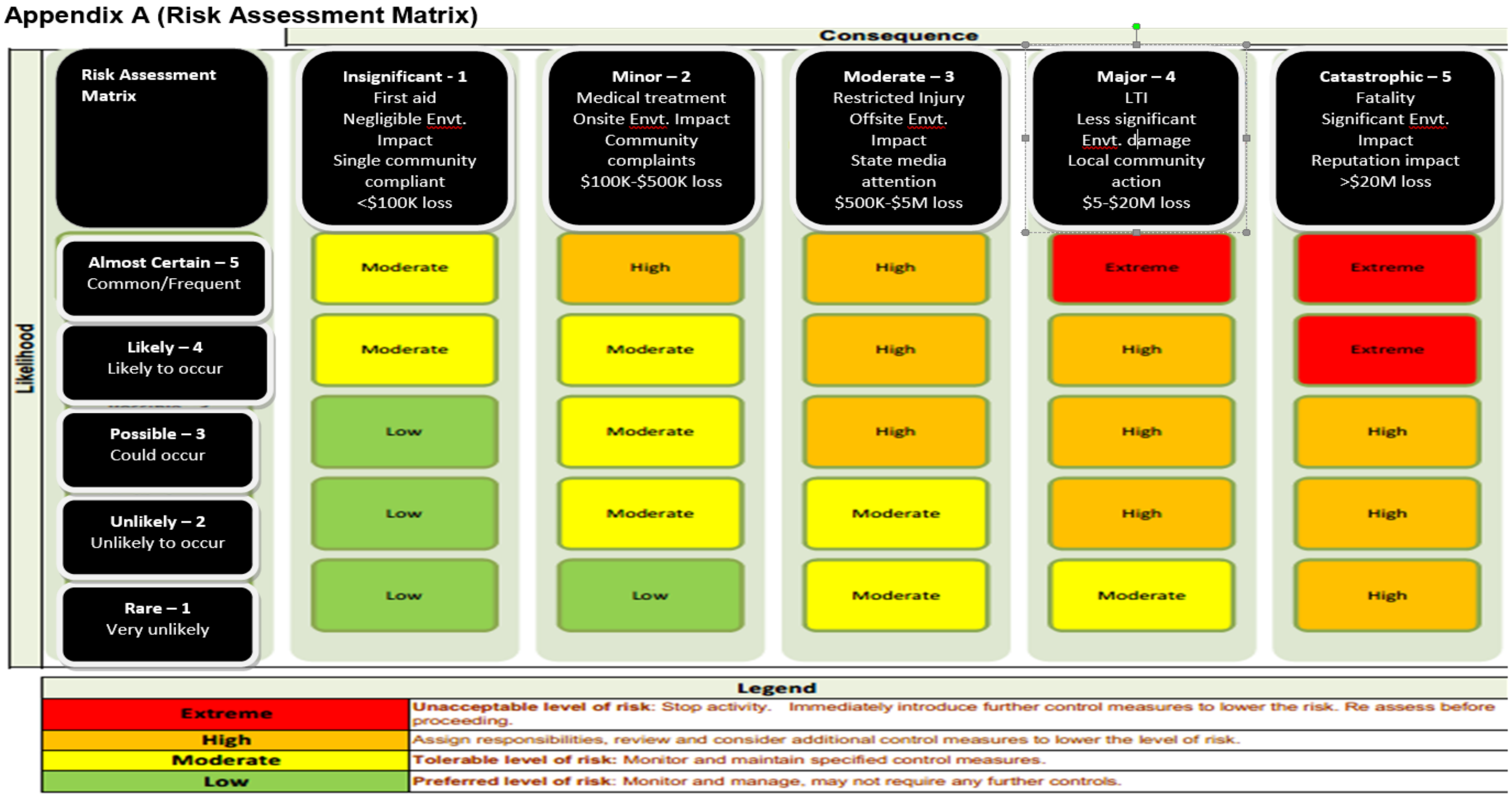


Almost Certain-5	Common or frequent occurrence. Likely to occur often during the life of an individual item or system, or very often in an operation of a large number of similar items.	Catastrophic-5	***Health & Safety* -** Fatality or permanent disability ***Environment* -** Impact with potential for severe long-term harm or impact on area of significance ***Community* -** International repercussions to reputation ***Financial loss* -** > $20M
Likely-4	Is known to occur or has happened. Likely to occur several times in the life of an individual item or system, or often in an operation of a large number of similar items.	Major-4	***Health & Safety* -** Lost time injury or illness ***Environment* -** Events causing harm which cannot be immediately recovered ***Community* -** Local action that threatens production ***Financial loss*** - $5M - $20M
Possible-3	Could occur or 'I've heard of it happening'. Likely to occur sometime in the life of an individual item or system or will occur several times in the life of a large number of similar components.	Moderate-3	***Health & Safety*** - Restricted duties injury or illness ***Environment* -** Off-site impact with localised harm ***Community* -** Regional or state media attention ***Financial loss* -** $500K - $5M
Unlikely-2	Unlikely to occur, but possible to occur sometime in eh life of an individual item or system or can reasonably be expected to occur in the life of a large number of similar components.	Minor-2	***Health & Safety* -** Medical treatment injury or illness ***Environment*** - On-site events with no potential to cause local harm ***Community* -** Repeated community complaints requiring management response ***Financial loss* -** $100K - $500K
Rare-1	Practically impossible, very unlikely to occur in the life of an individual item or system, or it may be possible, but unlikely to occur in the life of a large number of similar components.	Insignificant-1	***Health & Safety* -** First aid injury or illness not requiring treatment ***Environment* -** Single on-site event causing negligible harm ***Community* -** Single community complaint handled locally ***Financial loss* -** <$100K

Table 1. Likelihood and consequence ratings

Table 2. Risk Matrix

The risk rating of a risk is made by cross referencing the likelihood rating and the consequence rating using the risk matrix in table below:



Appendix A (Risk Assessment Matrix)

Likelihood	Consequence				
Risk Assessment Matrix	**Insignificant - 1** First aid Negligible Envt. Impact Single community compliant <$100K loss	**Minor – 2** Medical treatment Onsite Envt. Impact Community complaints $100K-$500K loss	**Moderate – 3** Restricted Injury Offsite Envt. Impact State media attention $500K-$5M loss	**Major – 4** LTI Less significant Envt. damage Local community action $5-$20M loss	**Catastrophic – 5** Fatality Significant Envt. Impact Reputation impact >$20M loss
Almost Certain – 5 Common/Frequent	Moderate	High	High	Extreme	Extreme
Likely – 4 Likely to occur	Moderate	Moderate	High	High	Extreme
Possible – 3 Could occur	Low	Moderate	High	High	High
Unlikely – 2 Unlikely to occur	Low	Moderate	Moderate	High	High
Rare – 1 Very unlikely	Low	Low	Moderate	Moderate	High

Legend	
Extreme	**Unacceptable level of risk**: Stop activity. Immediately introduce further control measures to lower the risk. Re assess before proceeding.
High	Assign responsibilities, review and consider additional control measures to lower the level of risk.
Moderate	**Tolerable level of risk:** Monitor and maintain specified control measures.
Low	**Preferred level of risk**: Monitor and manage, may not require any further controls.

Please see next page for detailed description of “Consequence” and “Likelihood” categories.

Treat the risks

8.9 The risk rating will identify the appropriate response action required to treat the risk.

Extreme risk	A risk where the activity requires immediate action. Identify and implement risk reduction measures immediately. Active monitoring and re-evaluation of the risk and reduction measures is required frequently.
High risk	A risk where the activity would be discontinued as soon as reasonably practical. Formal assessment rates these risks among the top immediate priorities for the Group. Monitoring and re-evaluation of the risk and reduction measures is required regularly.
Moderate risk	A risk where the exposure can be accepted in the short term (i.e. up to six months) with compensating controls to ensure the risk does not escalate. Formal assessment rates remediation actions as requiring short term attention. Evaluation of the risk and reduction measures is monitored at least every three months.
Low risk	A risk where the exposure can be accepted with compensating controls to ensure the risk is managed and does not escalate. Formal assessment rates remediation actions as requiring medium term attention. Monitoring and re-evaluation of risk measures and management controls is recommended at least every three months.

Table 4. Risk matrix and risk rating definitions

8.10 A target risk rating, no greater than Moderate, should be identified based on the risk appetite and risk tolerance statements. This is included in the risk register.

8.11 A risk owner must be identified and added to the risk register. A risk owner has primary responsibility and accountability for the risk. Where multiple stakeholders or jurisdictions are identified care must be taken to identify a risk owner with appropriate seniority and authority.

8.12 The risk owner and any relevant stakeholders should develop treatments for the risk. Some treatments may be relevant to multiple risks and some existing risk treatments may already be in place. Ensure these treatments are also included in the risk register.

8.13 Treatments should reduce the likelihood of the risk occurring and/or the consequence of a risk event. The **residual risk** rating is to be calculated as per the method above and entered into the risk register.

8.14 A date for outstanding treatments to be implemented, and/or a review date, should be entered into the risk register. Any outstanding treatments that are yet to be implemented are added to a risk treatment plan.

9. Monitor and review

9.1 Treatments on a risk treatment plan are to be reviewed for progress of their implementation quarterly until completion. Treatments on a risk treatment plan are to be reviewed for progress of their implementation quarterly until completion.

9.2 Completed treatments are closed and removed from the risk treatment plan before being updated on the risk register.

10. Measuring risk management performance

10.1 The measurement of risk management performance within the Group will involve internal and external audit activities.

10.2 Compliance reporting will monitor elements of the policy and framework that, if not carried out, can have significant impact on the enterprise risk management framework:

Requirement	Key Performance Indicator	Measure and Target
Risk awareness training.	The number of staff that have received risk awareness training.	95% of staff have completed risk awareness training.
Operational and project risks reviewed regularly.	Operational risk registers are reviewed every 6 months or upon an incident occurring. Project risks are reviewed as per project plan.	At least one forum/meeting addressing risks every three months or upon an event occurring (or less for projects).
Operational and project risk registers are in the correct format.	All risk registers are in the correct format.	100% of risk registers are in required format.
Audit findings are completed in a timely manner.	All actions to address audit findings are completed on, or before, the implementation date.	100% of actions are completed prior to implementation date.

Table 5. Performance monitoring metrics

11. Periodic review and continuous improvement

11.1 The Group will periodically review its risk appetite and risk tolerance in concert with its strategic risks. This will occur in line with the scheduled review of the Corporate Plan.

11.2 In preparation for Audit and Risk Management Committee meetings, all of the Group's risk registers are reviewed by staff and the SMT.

11.3 Recommendations from risk reviews, audit findings and consultation will be considered for action in order to continuously reduce the Group's exposure to risk. Action plans will be developed for implementation as part of the quarterly operational risk review.

Dictionary

12.1 In this Policy, Framework and in the Australian Standards:

‘Consequence’ means the outcome of an event impacting objectives.
‘Control’ means a measure that is modifying the likelihood or consequence of a risk.
‘Event’ means the occurrence or change of a particular set of circumstances.
‘Inherent risk’ means the amount of initial risk that exists, as best as can be estimated, before controls are introduced to mitigate the risk
‘Likelihood’ means the chance of something happening
‘Residual risk’ means the amount of current risk remaining after risk the controls are applied.
‘Risk’ means the effect of uncertainty on objectives. The effect is a deviation from the expected – positive or negative. It is characterised by reference to likelihood and impact.
‘Risk acceptance’ means the informed decision to accept a particular risk.
‘Risk treatment plan’ means the template to plan, initiate and monitor progress on risk treatments introduced to bring inherent risks to an acceptable level and must be used for all strategic risks and operational risks with a residual risk rating of Extreme or High. A risk treatment plan may be used to further manage lesser rated risks.
‘Risk appetite’ means the amount and type of risk that the Group is willing to pursue or retain.
‘Risk assessment’ means the overall process of risk identification, analysis, and evaluation.
‘Risk management’ means the coordinated activities to direct and control the Group’s activity with regard to risk.
‘Risk owner’ means the person with the accountability and authority to manage a risk.
‘Risk register’ means the record of information about identified risks.
‘Risk reporting’ means the form of communication intended to inform internal / external stakeholders on current state of risk management.
‘Target risk’ means the ideal residual risk rating after the treatments are applied and become controls.
‘Treatment’ means a future, planned, or not yet implemented control that is designed to modify a risk.