Risk Management Policy

TABLE OF CONTENTS

1. PURPOSE

Risk is defined in the Australian Standard AS/NZ ISO 31000:2009 as the 'effect of uncertainty on objectives'. Risk is inherent in all business activities, and every employee of Macarthur Coal Ltd continuously manages risk.

Risk management is defined in the Australian Standard as 'coordinated activities to direct and control an organization with regard to risk'. This document sets out the overarching policy for managing risk at Macarthur Coal.

The Company recognises that the aim of risk management is not to eliminate risk totally, but rather to provide the structural means to identify, prioritise and manage the risks involved in all our activities. It requires a balance between the cost of managing and treating risks and the anticipated benefits that will be derived.

Macarthur Coal acknowledges that risk management is an essential element in the framework of good corporate governance, and is an integral part of good management practice. The intent is to embed risk management in a very practical way into business processes and functions via approval processes, review processes and controls to add significant value to the Company; it is not to impose risk management as an extra requirement, which adds no value to the Company.

1.1 OBJECTIVES

The Risk Management Policy (the Policy) aims to ensure that the activities of Macarthur Coal Ltd and its controlled entities (Macarthur Coal) are undertaken within Board approved risk appetite and tolerance levels to protect the profitability, balance sheet and reputation of Macarthur Coal.

Embedding risk management principles and practices into strategy development and day-to-day operational processes is critical to achieving robust and proactive business outcomes – a balance between mitigating threats and exploiting opportunities. This Policy establishes the top-level framework for risk management at Macarthur Coal.

1.2 BACKGROUND

Macarthur Coal has developed a Risk Management Policy (the Policy) designed to protect and enhance resources and enable the achievement of its objectives.

The Policy emphasises that risk management is an integral part of Macarthur Coal's business processes.

The Policy is based on the following principles. Risk management is:

- the responsibility of the Board, all executives, managers, employees and contractors
- integrated into all business activities and systems
- based on the Australian Standard AS/NZ ISO 31000:2009, and
- compliant with ASX Principle 7 (reproduced Appendix 9.2).

A structured risk management framework provides a number of beneficial outcomes by:

- enhancing strategic planning through the identification of threats to the Macarthur Coal's Vision and strategic goals

- encouraging a proactive approach to issues likely to impact on the strategic and operational objectives of the Company
- improving the quality of decision making by providing structured methods for the exploration of threats and opportunities, and allocating resources.

2. SCOPE

The Policy applies to all Directors, officers, employees and contractors of Macarthur Coal Limited and its controlled entities (the Company; Macarthur Coal; MCC).

Where more detailed risk management policies or procedures are developed to cover specific areas of the Company's operations (e.g. insurance, occupational health and safety, commercial activities) they should comply with the broad directions detailed in the Policy.

3. POLICY

The Policy covers the following areas:

- Commitment to Risk Management
- Risk Management Framework
- Risk Governance
- Linking Risk Management and Strategy
- Risk Registers
- Internal Audit Process
- Risk Reporting
- Risk Management Continuous Improvement
- Crisis Management

3.1 COMMITMENT TO RISK MANAGEMENT

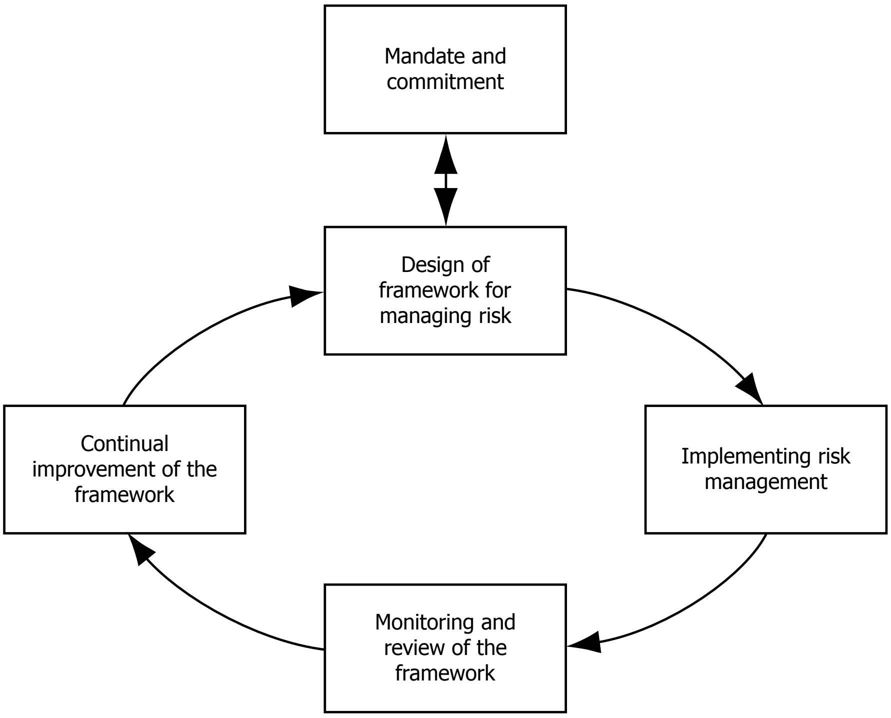
The Board and management of Macarthur Coal are committed to the implementation and maintenance of a formal risk management system, including the integration of risk management throughout the organisation, which is fundamental to the Company achieving its strategic and operational objectives.

3.2 RISK MANAGEMENT FRAMEWORK

The Australia/New Zealand Risk Management Standard AS/NZS ISO 31000:2009 forms the basis of the Policy. The Policy provides the foundations and organisation arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout Macarthur Coal. Figure 3.1 illustrates this framework diagrammatically.

The application of this standard is explained in the Risk Management Methodology set out in Appendix 9.1.

Figure 3.1: AS/NZS ISO 31000 risk management framework



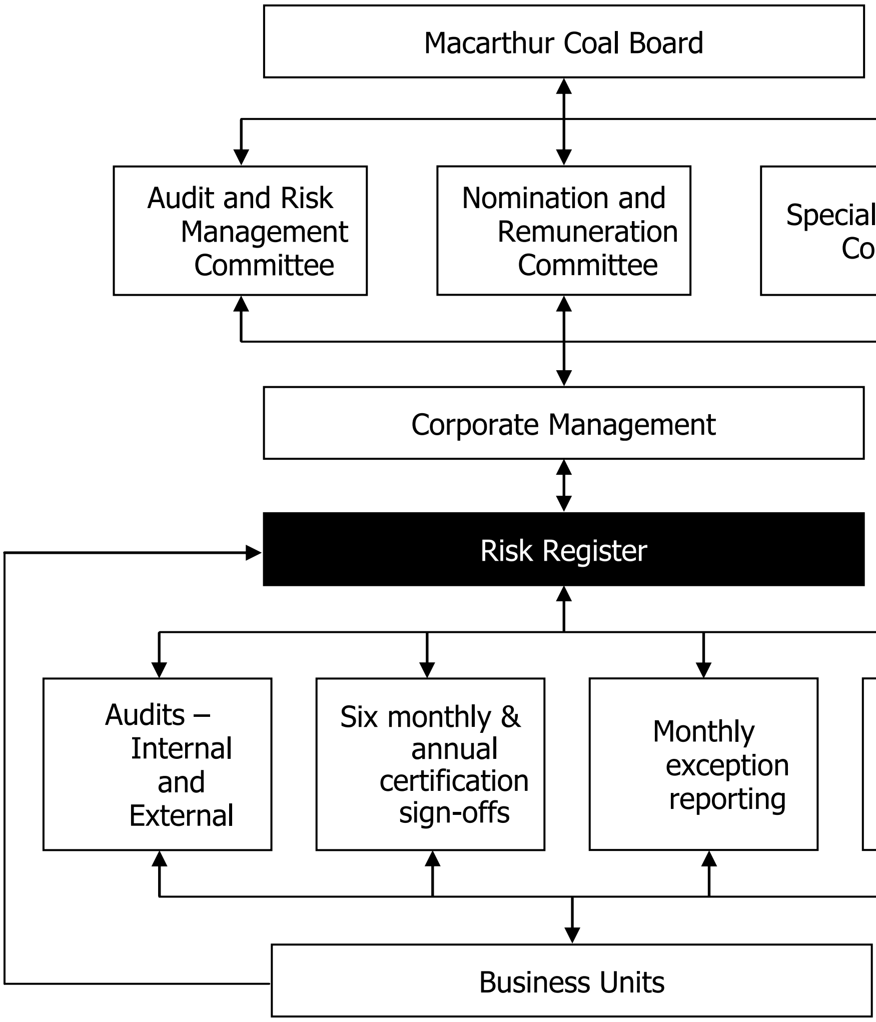
3.3 RISK GOVERNANCE

An effective risk management system is dependent on a governance structure that has:

- roles and responsibilities defined
- adequate separation of duties
- proper systems of supervision and monitoring of activities and transactions
- risk consciousness and a proactive approach to managing risks across the structure.

Figure 3.2 provides an overview of Macarthur Coal's risk governance structure.

Figure 3.2: Risk Governance Structure



The Board

The Board retains the ultimate responsibility for risk management and for determining the appropriate level of risk that Macarthur Coal is willing to accept. The role of the Board with respect to risk management encompasses both compliance and performance aspects:

- compliance:
    - allocate resources to implement and maintain the risk management process
    - delegate authorities and responsibilities
    - monitor the organisation's performance having regard for its risk appetite and risk management processes
    - review the ongoing effectiveness of the risk management process in achieving the organisation's objectives

- performance:
  - agree the risk appetite of the organisation having regard for the risk environment in which the organisation operates
  - review the organisation's risk profile against its agreed strategy ensuring that they are aligned and within the agreed risk appetite
  - set the risk policies setting out the internal framework for risk management across the organisation
  - set the 'tone at the top' for the organisation including endorsing and adopting the Company's Code of Conduct.

Board Committees

The Board has formally appointed the following board committees to monitor the relevant affairs of Macarthur Coal on behalf of the Board:

- Audit and Risk Management Committee
- Nomination and Remuneration Committee
- Special Projects Committee.

Special committees are formed from time to time for specific events, for example capital raising, to enable the monitoring of processes.

Audit and Risk Management Committee

The Audit and Risk Management Committee (ARMC) comprises three members. A primary role of the Committee is to:

- Identify risk associated with business strategies and activities
- Advise the board of the level of risk acceptable to Macarthur Coal
- Monitor and review the effectiveness of the risk and control environment.

On at least an annual basis the ARMC reviews the structure and processes in place within each area controlled by each direct report to the CEO to identify and assess the risks. This review includes a review of the status of all significant risks together with a review of risk events which have occurred since the last review and the resolution of those issues.

Nomination and Remuneration Committee

The Nomination and Remuneration Committee comprises three members. The primary risk management role of this Committee is to:

- Assess the necessary and desirable competencies of Board members
- Review and make recommendations to the Board on appointment and removal of Directors
- Review the remuneration and performance objectives, including risk management objectives, of the CEO
- Review and approve the remuneration of senior managers.

The Committee will incorporate the risk management framework into its processes and procedures.

Special Projects Committee

The Special Projects Committee consists of three Directors. The primary risk management role of this Committee relates to its role in reviewing, analysing and providing guidance to management on special projects that may arise from time to time. The Committee's is also tasked with providing guidance and recommendations during pre-feasibility and feasibility stages of various projects and overseeing due diligence processes prior to recommendations being made to the Board for approval of a special project.

Further, the Committee is charged with reviewing all public disclosures related to its Charter including:

- ASX announcements
- the annual reports
- press releases.

Thus, the Committee is cognisant of risk and incorporates risk management it into its processes and procedures.

Chief Executive Officer

The CEO is responsible for the development and implementation of business strategies, budgets, setting performance benchmarks and creating a corporate culture compatible with the business objectives and risk appetite of Macarthur Coal. Specifically, the CEO's key accountabilities include:

- ensuring that a robust MCC strategy is developed, regularly reviewed by management, discussed and approved by the Board and communicated, as appropriate, within the company and with external stakeholders
- taking overall responsibility for implementing the agreed strategy to achieve the corporate-wide goals and KPIs set in the MCC strategy
- reviewing on a regular basis and holding accountable the CEO's direct reports for the performance of all the major divisions and units of the company in accordance with the corporate, business, project and other plans.

A strong, useable and effective risk management system underlies each of these key accountabilities.

Additionally, the CEO is required to ensure that a comprehensive control system is operating efficiently and effectively.

The CEO has overall responsibility for the management and reporting of risks and the implementation of risk management strategies and policies within Macarthur Coal as determined by the Board.

The Board has delegated to the CEO various risk limits and responsibility for the adherence to these risk limits.

The CEO promotes discussion amongst the senior management team of Macarthur Coal on risk issues, in particular the process of assessing and identifying risks and alternative options for the treatment of these risks in line with changing business conditions, market practices and prudential controls.

Chief Risk Officer

The Chief Financial Officer (CFO) reports directly to the CEO on the implementation, operations and effectiveness risk management system. The CFO is the Chief Risk Officer and is responsible for the development and implementation of all risk management processes and methodologies. As such the CFO will:

- lead the development, implementation and management of the Macarthur Coal risk framework in accordance with the applicable Australian Standards for risk
- ensure that risk evaluation, monitoring, review and documenting occur in accordance with the Risk Management Policy and Methodology
- provide advice to the Board to ensure compliance with relevant legislation, regulations, policies and standards and to build Macarthur Coal's capability to mitigate risk related to human, financial and physical resources
- produce a consolidated Risk Register approved by the CEO for submission biannually to the Audit and Risk Management Committee for review of limits of acceptable risk
- update the Risk Profile Matrix, which provides an overview of risks and potential liability. The Risk Profile Matrix is submitted to the ARMC with the consolidated Risk Register.

Additionally, the CFO is required to ensure that a comprehensive financial control system is operating efficiently and effectively.

Management

Management concerns itself with issues relating to the general operation of Macarthur Coal as a whole and specifically with the operation and performance of activities under their direct control.

Management has a mandate to ensure risks are contained within approved risk tolerance levels and managed in accordance with Macarthur Coal's Risk Management Policy.

Management has responsibility for ensuring there are adequate operating procedures and practices in place to identify, assess and manage risk in their direct areas of responsibility and test control systems for effectiveness and relevance. Additionally, management has responsibility to be generally involved in the management and treatment of risk throughout Macarthur Coal.

The CEO's direct reports are responsible for affirming the accuracy of the Risk Registers for their area of responsibility and the effectiveness and on-going existence of risk mitigations to the CEO and the ARMC.

Management is to hold risk management meetings at least biannually to discuss risk developments and initiatives to mitigate risk.

Management's role with respect to risk management comprises:

- allocating resources to implement the agreed risk mitigation strategies on an ongoing basis
- developing and implementing systems to detect and report all risk events
- providing ongoing education and training in skills required to manage risk
- providing leadership in implementing and maintaining a structured risk management process to indentify, assess and manage risks
- developing the enterprise-wide and strategic risks and mitigation strategies

- agreeing the level of individual residual risks having regard for the agreed organisation risk profile
- ensuring the risk profile is aligned with strategy
- monitoring the major risks and risk events to ensure that risks are being properly identified and managed in accordance with the approved risk profile
- monitoring the ongoing effectiveness of the risk management process
- mapping the risk environment of the Company
- drafting and recommending the appropriate risk management structure
- supporting the Board in setting the 'tone at the top', including endorsing and adopting the Company's Code of Conduct.

Employees and Contractors

It is the responsibility of all Macarthur employees and contractors to:

- be aware of those aspects of the risk management system that are immediately relevant to their jobs. In particular, to be aware of and act in accordance with all policies, procedures, guidelines and work practices related to risk within their area of responsibility
- comply with all legislative, regulatory and Company policies and communicate any breaches promptly and accurately to the appropriate supervisor or manager
- report to their immediate supervisor or manager any real or perceived risks to the health, safety and working environment of themselves, their peers or the general public
- report to their immediate supervisor or manager any real or perceived risks that may significantly affect the profitability, performance or reputation of Macarthur Coal or that may leave the Company exposed to legal or regulatory action
- look for opportunities to improve operational efficiencies, optimise outcomes and minimise risk.

All employees are responsible for the ownership of, and for undertaking their part in, the actions and requirements of Risk Action and Mitigation Plans.

3.4 LINKING RISK MANAGEMENT AND STRATEGY

Embedding risk management principles and practices into strategy development as well as day-to-day operational processes is critical to achieving robust and proactive business outcomes – a balance between mitigating threats and exploiting opportunity.

As a general principle, the risk management process is to be undertaken in conjunction with strategic planning. The risks identified and evaluated as part of the strategic planning process will be the risks that will affect the entire Company and its ability to achieve its Vision.

Risk Registers are the primary mechanisms to bring corporate, business and operational/functional strategies, as articulated in the hierarchy of strategic plans, together to ensure appropriate risk minimisation plans are built into strategic implementation plans. The figure below illustrates how this occurs.

Figure 3.5: Linking Risk, Strategy and Performance

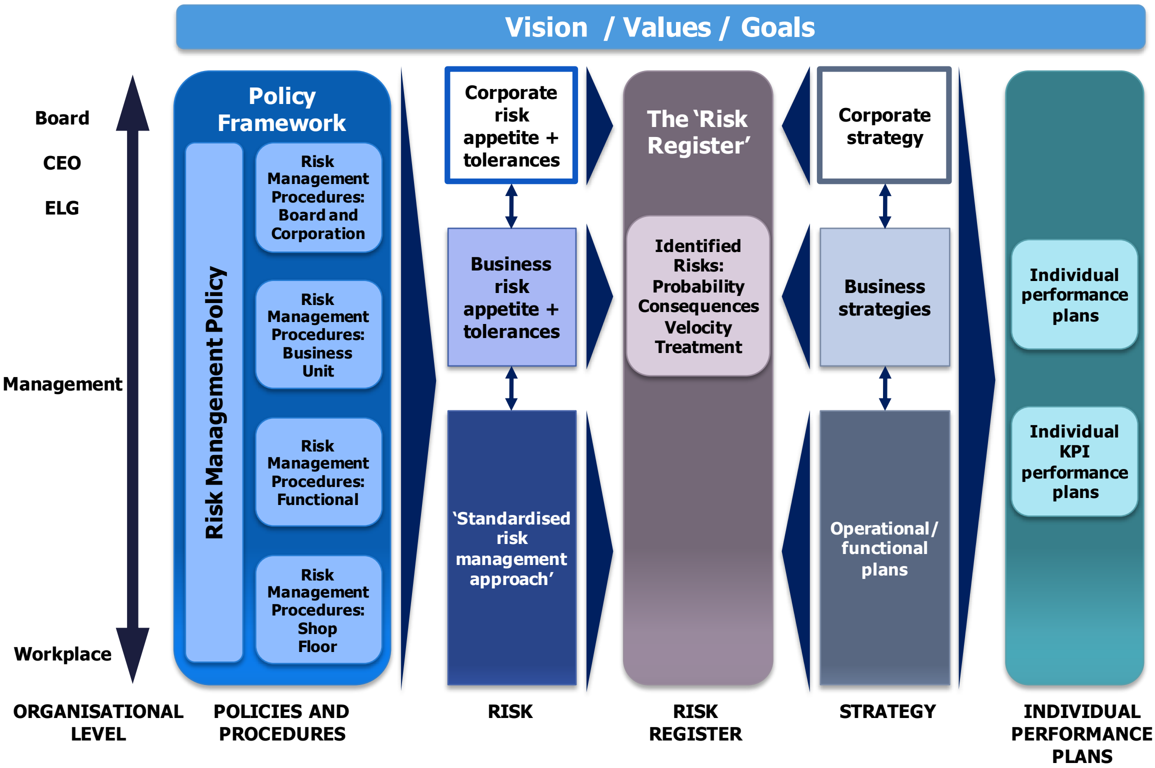


Figure 3.5 makes several key statements about risk management in Macarthur Coal. First, the Company's Vision, Values and Goals have a major impact on Macarthur Coal's risk and strategy frameworks. Our acceptance and rejection of risks all flow back to our Vision for the Company, 'The Number One Independent Coal Company', as well as the four Macarthur Coal values of:

- value people
- work together
- lead the way
- talk straight
- our corporate goals as set out in the Corporate Strategic Plan.

Second, our risk management system needs to be integrated from the boardroom to the shop floor. We have different levels of risk, ranging from overall corporate risks such as the positive and negative impacts of making large investment decisions through to the risks associated with operating a particular piece of equipment at a particular site. Our risk management system needs to allow an integrated and linked process of managing all these risks and reporting on these risks.

To this end, this policy framework needs to be companywide, able to be applied from the boardroom to each job site. To achieve this, the Risk Management Policy will be supplemented with a series of Risk Management Procedures. Each Risk Management Procedure will be relevant to the particular scope of operation to which it applies.

Third, the actual risk identification, risk analysis, risk evaluation and risk treatments will vary depending on the level of the organisation at which the risk occurs. For example, the Board will maintain a corporate risk appetite and risk tolerance document. For each major division of the business, there will be business division risk appetite and tolerances. At each work unit, there will be a series of standardised risk management processes. Some of these risk management procedures will be based on specific standards. For example, *AS/NZS 3760:2010: In-service safety inspection and testing of electrical equipment*. Others will be based around the operating manuals for specific pieces of equipment.

Fourth, the integrating feature of both the different levels of policies as well as the link between risk management and strategy is the Risk Register. The Risk Register is the means of recording risk management processes for identified risks. We intend to move to a system of an integrated Risk Register which allows the entering of risks and the reporting on risks at the different levels in the Company.

Fifth, this Risk Register will also be linked to the strategic processes of the Company. We currently have under development an integrated approach to strategy and strategic planning which commences with the overall corporate strategy and then proceeds to have a linked series of more detailed plans. At each level of planning, the strategies developed must be linked back to the risks identified for that level of the Company. Undertaking a risk identification/analysis/evaluation process can assist in the development of plans at all levels of Macarthur Coal. The Risk Register will contain a cross reference to the specific strategies which discuss and address the risk.

Finally, we are moving to integrate the personal planning and KPIs with the strategic plans and their KPIs as well as the corresponding risks and Key Risk Indicators (KRIs). In this way we plan to have an integrated series of three management systems underlying the Company. These are:

- the risk management system
- the strategic planning and implementation system
- the performance management system for personnel.

3.5 RISK REGISTERS

The Risk Register is currently comprised of a series of unrelated spreadsheets across a combination of business units and risk types. The Company's intention is to move to an appropriate integrated risk management platform that is robust, easy to use and capable of upwards scalability to meet the needs of the Company's Vision.

Each direct report to the CEO has responsibility for maintaining risk registers for his/her areas of responsibilities. The registers are to:

- use a system of unique Risk IDs that provide a linkage of risk to the Company's core strategies and functional business areas
- list the risks which could cause losses to be incurred and possible causes
- list the consequences
- provide an assessment of the inherent risks
- detail the existing risk mitigators
- provide an assessment of the strength of the mitigators
- provide an assessment of the residual risks
- detail any action plans to reduce residual risks.

Whenever any functions or systems are developed or changed, or new strategies, products or projects are considered, management is required to carry out a risk appraisal. This review is carried out using the procedures and tools set out in the Macarthur Coal Risk Management Methodology. The respective Risk Register is to be updated accordingly.

3.6 INTERNAL AUDIT PROCESS

The Internal Audit function has been outsourced to one or more specialist audit services provider (Internal Auditor). The Internal Auditor carries out reviews of the various Company systems using a risk based audit methodology. The risk registers maintained by each direct report are the foundation for all audits.

The Internal Auditor is responsible to the ARMC and is charged with the responsibility for completing the agreed program of independent reviews of the major risk areas. The audit program is constructed having regard for the major risks of the business and the time since the last review was carried out on these risks.

The scope of the audit program also includes joint venture operations.

The Internal Auditor is responsible for reviewing the risks that have been identified, testing controls and following up to confirm that mitigation initiatives and recommendations have been implemented.

The Internal Audit function is the subject of an annual review by the ARMC having regard for information supplied by the external auditors and management as well as any third party, including regulatory authority reports.

3.7 RISK REPORTING

Risk is reported in the following ways:

Board Reporting

Board meetings generally convene monthly. One function of monthly meetings is for the Board to be informed by management of current events, new developments and potential exposures to losses, as identified through the risk management system. In particular, the Board has a special role in reviewing, and when necessary, deciding on actions related to material business risks.

As defined by the ASX Corporate Governance Principles and Recommendations, material business risks means 'risks that could have a material impact on a company's business.' Material business risks are dealt with in standard board reports, which encompass marketing, operations, financial performance, investor relations and business development. Financial and production reports incorporate performance benchmarks. Significant deviations from benchmarks act as a mechanism to flag potential exposure to risk.

Board meetings are structured to involve management participation to allow Directors to obtain management's comments on matters likely or capable of affecting Macarthur Coal's financial position or future performance.

Assessment of Effectiveness

On a six-monthly basis the Board will, on the advice of the ARMC, receive the certification provided by the CEO and the CFO as to the effectiveness in all material respects of the risk management and internal control system in relation to material business risks.

Business Unit Managers will provide a six monthly certification that risks have been managed in line with this Policy. At the year end and half year, each Business Unit completes an internal control questionnaire; this is signed by the Business Unit Manager. The Company Secretary will provide a consolidated exceptions report to the ARMC and Board on a six-monthly basis, reflecting the current Business Unit certifications and a summary of any major changes since the last report.

The certification process is outlined in Appendix 9.5.

Internal Audit Reporting

The Internal Auditor provides the ARMC with a report after completing its work program as per the scope of work agreed between the Internal Auditor, business unit management and the ARMC.

The report describes the review undertaken and tests performed, conclusions reached, corrective action plan, personnel responsible to take corrective action and completion dates.

Preparation of the report includes management's review to confirm accuracy of facts.

Copies of the report are provided to the CEO, CFO and Company Secretary. Relevant sections of the report are also provided to managers responsible for areas reviewed.

Statutory Compliance

Board reporting includes incident reporting as a standing item. Managers are required to forward to the Company Secretary all details of statutory and regulatory non-compliance, and ensure that letters and responses to regulatory authorities are maintained, and made available to the Company Secretary, if requested.

The relevant executive is given responsibility for tracking any matters through to completion.

Issues with the potential to affect the share price or financial performance of Macarthur Coal are reported at the earliest possible time to all Board members.

Assurance Reporting

ARMC reporting includes half-yearly assurance reports on investigations into non-compliances. Managers are required to provide the CRO's nominated manager with updates on investigations into non-compliances and remedial action being taken to address risks relating to non-compliance.

Risk Mitigation Action Plans

Actions to improve risk mitigation are documented in the Risk Register. The CRO is to monitor the progress of implementing mitigating initiatives and reporting progress to the ARMC.

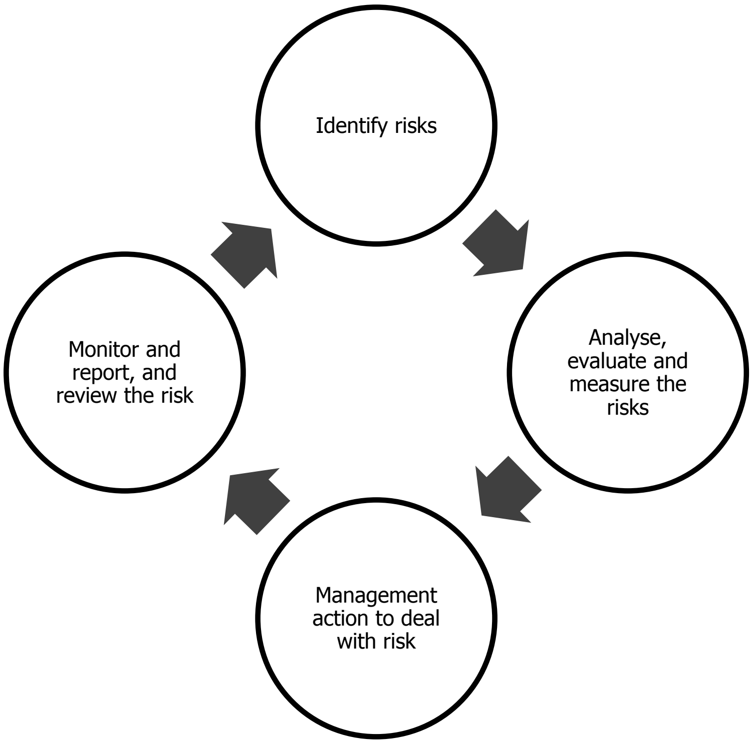
3.8 RISK MANAGEMENT CONTINUOUS IMPROVEMENT

Macarthur Coal assesses the effectiveness of its Risk Management Framework through a well-structured continuous improvement process to ensure risks and controls are continually monitored and reviewed. This includes appraisal of actions taken by risk owners to manage risks, input from the Internal Auditor and other assurance processes.

The Risk Management Methodology is aligned with the principles of continuous improvement. It requires management to continually identify, assess, mitigate, review and report risks within their business units so that all risks are mitigated and managed to an acceptable level in accordance with Macarthur Coal's risk appetite statement.

The diagram below illustrates the continuous improvement cycle in relation to risk management.

Figure 3.6: Risk Management Continuous Improvement Cycle



3.9 CRISIS MANAGEMENT

The ability to react effectively at an operational and strategic level to crisis events forms a subset of the Macarthur Coal risk management framework. The Company's approach is outlined in the Crisis Management Manual and Procedures, which incorporate emergency response, strategic response, disaster recovery, and business continuity planning.

4. DEFINITIONS

Term	Definition
ARMC	Audit and Risk Management Committee
Australian Standard	Means the Australia/New Zealand Risk Management Standard AS/NZS ISO 31000:2009, which forms the basis of Macarthur Coal's risk management methodology.
Board	Means the Board of Directors of Macarthur Coal Limited.
Chief Executive Officer (CEO)	Means the person appointed by the Board to manage Macarthur Coal on a day-to-day basis. The CEO reports directly to the Board.
Chief Financial Officer (CFO)	Means the person appointed as Chief Financial Officer of the Company and includes any person appointed to perform the duties of the Chief Financial Officer.
Chief Risk Officer (CRO)	Means the person appointed under this Policy as the Chief Risk Officer of the Company and includes any person appointed to perform the duties of the Chief Risk Officer.
Company	Means Macarthur Coal Limited.
Company Secretary	Means the person appointed as Secretary of the Company and includes any person appointed to perform the duties of Secretary.
Consequence	Outcome or impact of an event and may be expressed qualitatively or quantitatively. There can be more than one consequence from one event. Consequence can be positive or negative. Consequences are considered in relation to the achievement of objectives.
Constitution	Means the Constitution of Macarthur Coal Limited, which forms the rules that apply to the Company as altered or added to from time to time.
Control	Measure to modify risk. Term often used interchangeably with risk 'treatment'. Specifically, controls are the result of risk treatment. Controls include any policy, process, device, practice or other actions designed to modify risk. See Risk Treatment.
Director	Means a person or elected from time to time to the office of Director of the Company in accordance with the Constitution and includes any Alternate Director duly appointed as a Director.
ELG	Means the Executive Leadership Group of Macarthur Coal Limited.
Event	The occurrence of a particular set of circumstances. The event can be certain or uncertain. The event can be a single occurrence or a series of occurrences.
Exposure	Extent to which the Company is subject to an event.
Inherent risk	The intrinsic risk prior to considering any controls in place.
Likelihood	General description of probability or frequency. It can be expressed qualitatively or quantitatively.
Material business risks	As defined by the ASX Corporate Governance Principles and Recommendations, material business risks means 'risks that could have a material impact on a company's business.'
Management	Means the executive management of the Company.

Term	Definition
Regulatory authority	Federal, state or local agency that has a legal and/or regulatory power over an aspect of the Company's activities including the capacity to initiate prosecutions. For example, there are specific Safety and Mining Regulators for each State and Territory in Australia.
Residual risk	The level of risk that remains after assessing the effectiveness of the controls, management strategies and other mechanisms currently in place to mitigate a particular risk.
Risk	Risk is the exposure to unexpected financial or other damage arising from Macarthur Coal's business activities. The risk elements comprise market, liquidity, credit, operational, legal, compliance and reputation risks.
Risk acceptance	Informed decision to take a particular risk. Risk acceptance can occur without risk treatment or during the process of risk treatment. Risks accepted are subject to monitoring and review.
Risk analysis	The systematic process applied to understand the effect of the uncertainty of the risk on the Company's goals and objectives.
Risk appetite	The Company's approach to assess and eventually pursue, retain, take or turn away from risk.
Risk assessment	The overall process of risk identification, risk analysis and risk evaluation.
Risk avoidance	A decision not to become involved in, or to withdraw from, a risk situation.
Risk evaluation	Process of comparing the level of risk against risk criteria. Risk evaluation assists in decisions about risk treatment.
Risk identification	The process of determining what might happen, how, when and why.
Risk management	Risk management is the culture, processes and structures that are directed towards realising potential opportunities while managing adverse effects.
Risk management framework	Set of elements of an organisation's management system concerned with managing risk. Management system elements at Macarthur Coal include strategic planning, decision making, and other strategies, processes and practices for dealing with risk.
Risk Management Methodology	The methodology for the identification, analysis, assessment, mitigation and monitoring of risks is set out in the Risk Management Methodology which is provided as Appendix 9.1.
Risk management plan	Document within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk. Management components typically include: procedures, practices, assignment of responsibilities and sequence of activities.
Risk management policy	Statement of the overall intentions and direction of the Company related to risk management.

Term	Definition
Risk management process	The systematic application of management policies, procedures and practices to the tasks of communicating, establishing the context, identifying, analysing, evaluation, treating, monitoring and reviewing risk across all functions within Macarthur Coal. The process is supported by the Board and all personnel.
Risk mitigation	Measures taken to reduce an undesired consequence.
Risk owner	The person specifically assigned to manage the risk, including monitoring the risk, its controls and any treatments that are implemented.
Risk register	Document used for recording risk management processes for identified risks. Data recorded in the risk register(s) provides summary information for the Company's risk profile.
Risk tolerance	The acceptable variation relative to the achievement of an objective.
Risk tolerance level	Risk tolerance level is the level of acceptable risk exposure in respect of each identified risk approved by the Board.
Risk treatment	The process of selection and implementation of measures to modify risk.
Stakeholders	Those people and organisations who may affect, be affected by, or perceive themselves to be affected by a decision, activity or risk.

5. RESPONSIBILITIES

5.1 POLICY MANAGEMENT

The Risk Management Policy is a 'living' document that will be altered as required.

Approval of the Policy is vested with the Board.

Reviews of the Policy are the responsibility of the Policy Owner and will be conducted annually.

Advice and opinions on the Policy will be given by the Audit and Risk Management Committee.

5.2 POLICY IMPLEMENTATION

Implementation of this Policy is the responsibility of the CEO.

6. PROCEDURE

The Risk Management Policy is supported by the Risk Management Methodology set out in Appendix 9.1.

7. REFERENCES

The Risk Management Policy defines principles related to risk management, requiring management to develop, implement and maintain a structured and documented approach to risk management that is integrated within the day-to-day business activities.

The Risk Management Policy is part of a suite of policies developed to define the principles which management is required to adopt in directing and controlling Macarthur Coal's activities.

This Risk Management Policy is supported by, and linked to, specific Macarthur Coal policies and procedures as issued from time to time. As at the date of this Policy, these policies and procedures include, but are not limited to:

- Crisis Management Manual and Procedures
- Continuous Disclosure Policy
- Delegation of Authority Policy
- Segregation of Duties Policy
- Investments Policy applicable to Short Term Investments
- Foreign Exchange Hedging Policy
- Foreign Exchange Hedging Products Policy
- Interest Rate Hedging Policy
- Intercompany Internal Interest and Management Charges Policy
- Environment Policy
- Human Resources Policy
- Safety Policy
- Share Trading Policy
- Shareholder Communication Policy

- Treasury Policy
- Fraud and Corruption and Whistleblower Policy
- Codes of Conduct.

Appendix 9.3 overviews the policies listed above.

Strategy documentation includes, but is not limited to:

- Strategic Directions Document
- Corporate Strategic Plan.

Governance documentation includes, but is not limited to:

- Board Charter
- Audit Risk Management Committee Charter
- Nomination and Remuneration Committee Charter
- Special Projects Committee Charter.

8. DOCUMENT CONTROL MANAGEMENT

Refer to the Document Version Control Table on the final page of the Policy.

9. APPENDICES

- 9.1: Risk Management Methodology
- 9.2: ASX Principle 7 – Recognise and manage risk
- 9.3: Major Policies
- 9.4: Risk Register Template
- 9.5: Certification Process

9.1 RISK MANAGEMENT METHODOLOGY

Introduction

The Australia/New Zealand Risk Management Standard AS/NZS ISO 31000:2009 (the Australian Standard) forms the basis of our risk management methodology.

The Risk Management Methodology sets out the approved processes and tools to be used for the implementation and maintenance of an enterprise risk management system for Macarthur Coal.

Risk Management is applied across all of Macarthur Coal's functions enabling all classes of risk to be managed in an integrated manner. It is important to note that this does not mean adoption of uniform methods for all types of risk.

Why Do We Need Risk Management

The underlying premise for risk management is that all organisations exist to provide value for their stakeholders. All organisations face uncertainty and the challenge for the Board and management is to determine how much uncertainty the organisation is prepared to accept as it strives to grow stakeholder value.

Risk management enables the Company to operate more effectively in environments filled with risk. More specifically risk management allows the group to:

1. *Align the strategic direction to its risk profile*

   The development and execution of the group strategy will be worthless, and possibly even dangerous, if the risks involved in the strategy are not understood and those risks are not compatible with the group's desired risk profile.

2. *Allocate scarce resources*

   A good system of risk management can greatly assist in the most effective allocation of scare resources. The risks are prioritised which helps with the determination of the optimum utilisation of resources.

3. *Consistently monitor operations, ensuring a climate of 'no surprises'*

   A structured risk management process ensures that the risks of the business are fully understood by all personnel from operatives to the Directors. It makes it easier to monitor and report on the mitigation of these risks to the desired level. It also helps ensure a climate of 'no surprises' even though risk events will occur and losses associated with these risks be incurred.

4. *Have solid bases for decision making*

   When the risks associated with various alternate solutions are understood, the Board and management will be capable of making better quality decisions. Good risk management will ensure that decisions implemented will have acceptable levels of risk relative to growth and return objectives. Also, consideration of areas where risk can arise will highlight areas where opportunities for improvements exist.

5. *Satisfy regulators, markets, etc.*

   The existence of a proper system of risk management is a basic tenet of good corporate governance and is a recommended requirement for public companies quoted on the Australian Securities Exchange (ASX). It is a foundation for any continuous disclosure regime required by regulatory authorities including the Australian Securities and Investments Commission (ASIC).

Key Documentation

Details of conducting a risk management system in accordance with the Australian Standard, AS/NZS ISO 31000, are found in the following documents.

Details of conducting a risk management system in accordance with the Australian Standard, AS/NZS ISO 31000, are found in the following documents.

Table 1: Risk Management Standards and Guidelines

Catalogue No.	Title	Description
AS/NZS ISO 31000	Risk management – Principles and guidelines	The Australian Standard provides principles and generic guidelines on risk management. It can be used by any public, private or community enterprise, association, group or individual. Therefore, AS/NZS ISO 31000 is not specific to any industry or sector.
ISO Guide 73:2009	Risk management - Vocabulary	Supporting standard for AS/NZS ISO 31000. Provides the definitions of generic terms related to risk management.
ISO/IEC 31010:2009	Risk management - Risk assessment techniques	Supporting standard for AS/NZS ISO 31000. Provides guidance on selection and application of systematic techniques for risk assessment.
HB 327:2010	Communicating and consulting about risk	Provides guidance to individuals and organisations to understand communication and consultation when managing risk.
HB 436:2004	Risk Management Guidelines Companion to AS/NZS 4360:2004	A companion document to AS/NZS 4360 Risk Management. While this is related to the previous Australian Standard, it remains a useful guide to managing risks and contains information not included in the current standard or supporting documents.
HB 254-2005	Governance, risk management and control assurance	Guidelines on the implementation of a Control Assurance Plan, with an understanding of the relationship between governance frameworks and management practices.

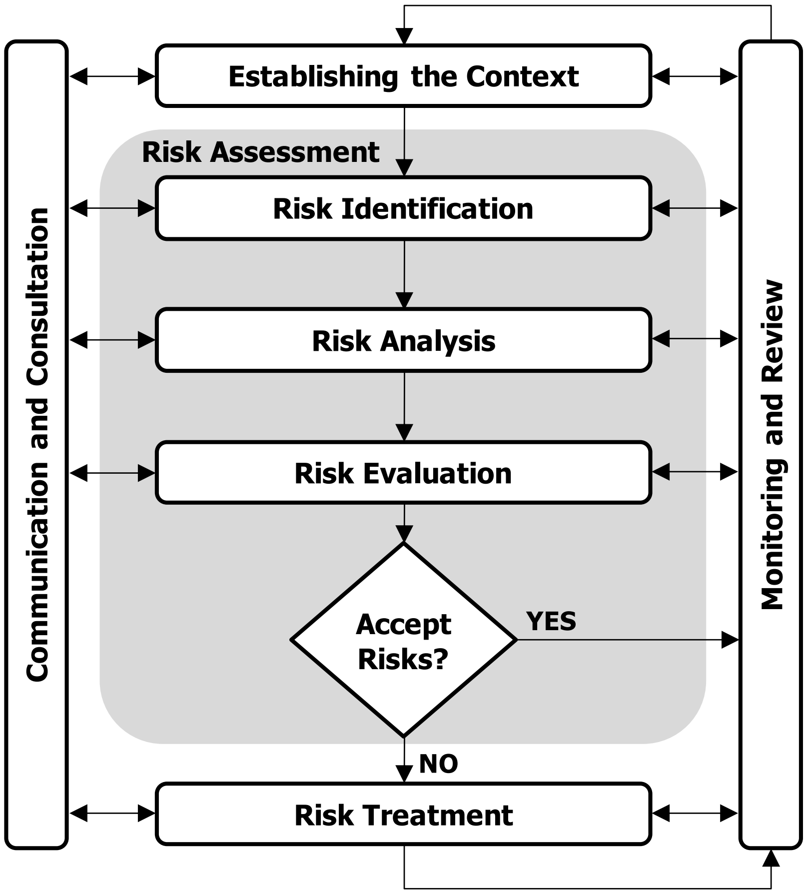
Catalogue No.	Title	Description
HB 158-2006	Delivering assurance based on AS/NZS 4360:2004 Risk Management	A guide for internal auditors and any other assurance provider such as external auditors, and safety, health and environmental auditors.
AS 3806-2006	Compliance programs	Provides guidance on the principles of effective management of an organisation's compliance with its legal obligations, as well as any other relevant obligations such as industry and organisational standards and principles of good governance.
AS/NZS ISO 9001:2008	Quality management systems - Requirements	Specifies requirements for quality management systems.
AS/NZS 5050:2010	Business continuity - Managing disruption-related risk	Describes the application of the principles, framework and process for risk management, as set out in AS/NZS ISO 31000:2009, to disruption-related risk. Managing such risk effectively will help maintain continuity of an organisation's business.
HB 221:2004	Business Continuity Management	Sets out a definition and process for business continuity management, and provides a workbook that may be used by organisations to assist in implementation.
AS/NZS4360: 2004	Risk management to manage occupational health and safety risks	Sets out requirements for an occupational health and safety management system.

Copies of these documents are available on request from the CRO.

Risk Management Process

The risk management process from the Australian Standard is outlined in Figure 1 below.

Figure 1: AS/NZS ISO 31000 risk management process



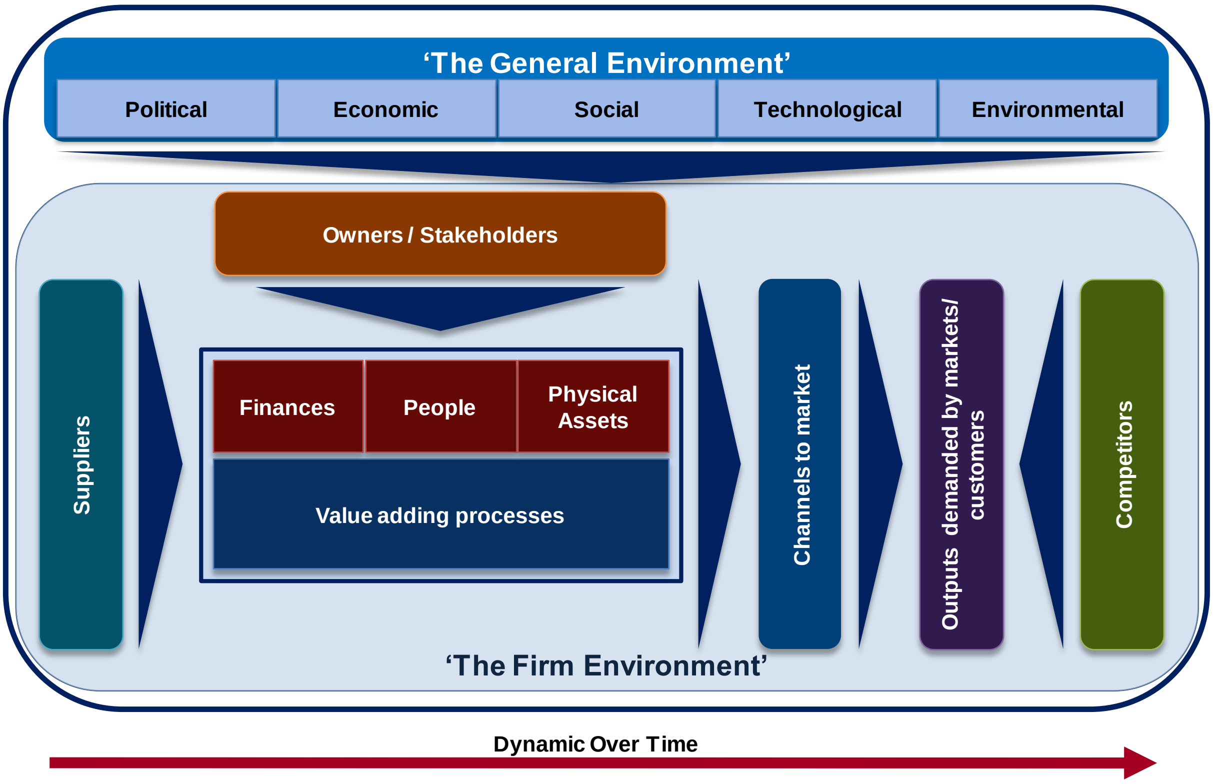
Step 1: Establishing the Context

(References: AS/NZS ISO 31000:2009, s. 5.3; IEC/FDIS 31010:2009, s. 5.2)

'By establishing the context, the organization articulates its objectives, defines the external and internal parameters to be taken into account when managing risk, and sets the scope and risk criteria' (AS/NZS ISO 31000:2009, p. 15).

The starting point to establish the risk context for Macarthur Coal is the overall environment in which the Company operates. This is shown diagrammatically in Figure 2 and summarised below.

Figure 2: Macro Framework to Identify Risk



The Company, together with the industry, is impacted by the macro forces of the 'general environment'. These are:

- political/regulatory environment
- economic environment
- social and demographic environment
- technological environment
- physical environment.

The industry or value chain is the next level of analysis. This involves identifying the risks inherent in the Company's:

- suppliers
- channels to market (both physical, e.g. rail, ports, shipping, as well as intermediaries such as agents)
- the risks emanating from the markets in which the product is sold and the risks associated with various segments of customers
- the risks present due to the actual or potential actions of competitors.

The next level of risk analysis is the Company itself. For risk purposes, the Company can be considered as the stakeholders and owners, whose requirements must meet and the value adding structure of the Company.

The value adding structure of the Company comprises the three resources available to the Company:

- people
- finance
- physical assets.

The other component of the Company from a risk perspective is the value adding stages the organisation undertakes in order to produce the products and services required by customers. In the case of Macarthur Coal, this can be considered as:

- the development processes required to develop a mine
- the process of mining and coal processing
- the systems which enable these value adding stages, e.g. human resource management, finance and accounting, etc.

Thus, the macro framework provides the overarching model to begin to establish the context for the identification and analysis of the risks facing Macarthur Coal.

As such, the initial step in the risk management process is to conduct an environmental review. This review is normally conducted as part of the business planning process. The completion of this review ensures that the risk management process is aligned with Macarthur Coal's strategic direction and considers the total environment in which Macarthur Coal operates.

There are a number of tools that can help to develop an understanding of the risks facing the Company. These include, but are not limited to:

- SWOT Analysis
- PESTE Analysis
- personal experience, corporate history, incident and events
- audits or physical inspections
- brainstorming
- questionnaires
- expert judgment.

Step 2: Identify Risks

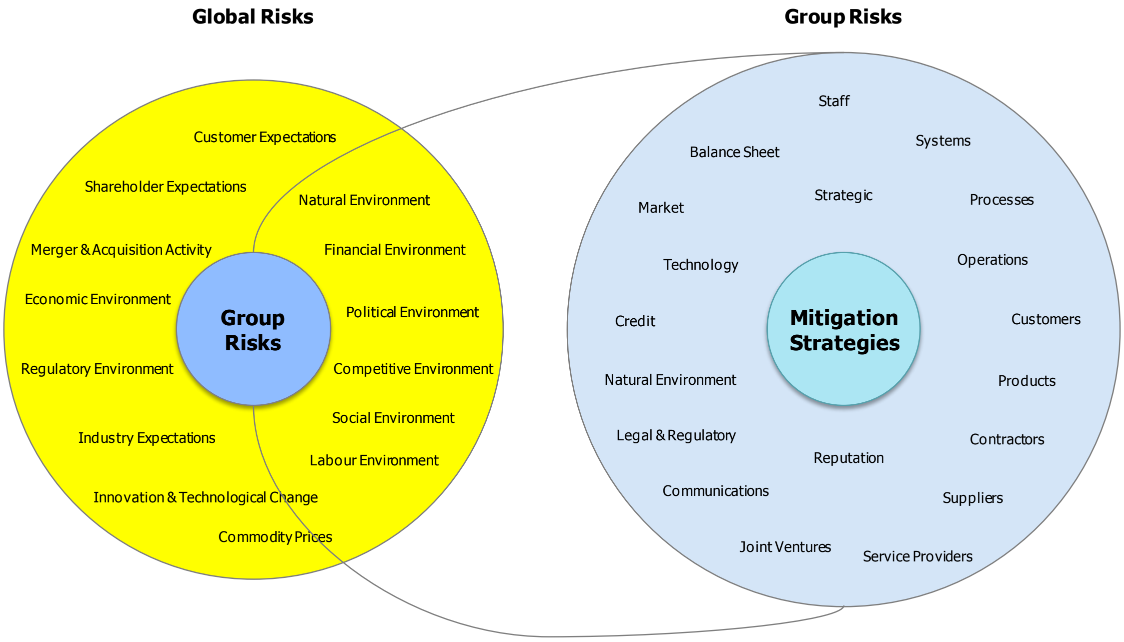
(References: AS/NZS ISO 31000:2009, s. 5.4.2; IEC/FDIS 31010:2009, s. 4.3.3)

'Risk identification is the process of finding, recognising and recording risks' (IEC/FDIS 31010:2009, p. 12).

Risks that could impact operations and events that would result in the risk occurring need to be identified during this phase of the risk management process. Since the risk management process defines risk as 'the effect of uncertainty on objectives' (AS/NZS ISO 31000:2009, p. 1), it is helpful to link Macarthur Coal's objectives to the risk identification.

To ensure that all risks have been considered, use the global and company risk areas set out in Figure 3 below.

Figure 3: Global and Group Risk Areas



The global risks which surround the group risks set out the uncertainties that have significant strategic impact on Macarthur Coal. Global risks are normally difficult to manage.

The group risks are those over which management exercises control and for which management implements specific mitigation actions.

It is critical in this analysis stage to ensure that the proper risks are identified and that risks are not confused with the triggers or the consequences.

A trigger is an event which can cause a risk to occur. A consequence is the impact on Macarthur Coal resulting from the risk event. There may be more than one trigger that can cause a particular risk occurrence, so it is important to identify all likely triggers.

Proper identification of the risks ensures that appropriate and cost effective mitigation measures can be applied.

If consequences are confused with risks, the mitigators of some of the likely consequences arising from a particular risk event could be excluded. Alternately, separate mitigators for the various risk consequences may be put in place at the expense of an overall risk mitigation strategy which could be more effective and less costly.

Techniques to be used to identify risks include:

- brainstorming
- history and failure analysis
- process mapping
- comparison with industry standards and practices.

Step 3: Analyse the Risks

(References: AS/NZS ISO 31000:2009, s. 5.4.3; IEC/FDIS 31010:2009, s. 5.3)

Level of risk = consequence x likelihood

Risk analysis is the process of calculating the likelihood of an event and consequence if it were to occur. The product of these two variables is the risk rating.

Thus, the consequences of each identified risk event need to be determined. When considering the consequences, both monetary and non-monetary consequences need to be considered.

The analysis is calculated initially on an 'inherent risk' basis; that is, the likelihood of the event occurring and the consequences of that event, if no mitigation strategies were put in place.

The triggers for each risk should also be determined. Some triggers may have more than one consequence; some consequences will apply to more than one trigger.

Use the generic consequence list set out in Table 2 below as a checklist to ensure that all outcomes have been addressed.

Table 2: Consequence List

Consequence
Revenue / margin loss
Loss of sales
Loss of production
Loss of customers
Loss of capital
Loss of funds
Loss of assets
Loss of licence
Increased costs
Write-off / write-downs
Penalties
Litigation / Judgment / Settlement Cost
Restitution / Compensation
Recovery Cost
Rework Cost
Cost of handling complaints
Injury / Stress Compensation Claims
Damaged reputation
Reduced share price

The next step requires an assessment of an Inherent Risk Rating.

The Inherent Risk Rating is based on the likelihood of the risk event occurring and the financial impact of the event.

Determining likelihood can be subjective, particularly where data are not available. However, historical data that take into account frequency of exposure and statistical data are often available and can be used to determine whether the likelihood of an event is:

- Almost certain
- Likely
- Possible
- Unlikely
- Rare

The likelihood of the risk occurring is linked to probabilities. The higher the probability, the higher the likelihood. The likelihood rating scale in Table 3 has been developed as a tool to assist with the Likelihood assessment.

Table 3: Likelihood Rating

Likelihood Rating	Likelihood	Frequency	Indicative Probability Range
5	Almost Certain	Risk is expected to materialise multiple times over a 1 year period	>95%
4	Likely	Risk is expected to materialise once in a 1 year period	75-95%
3	Possible	Risk is expected to materialise once in a 5 year period	25-75%
2	Unlikely	Risk is expected to materialise once in a 25 year period	4-25%
1	Rare	Risk is expected to materialise less often than once in a 25 year period	<4%

The impact of the risk event requires an assessment of the highest cost outcome, taking into account ancillary costs as well as direct costs that will be incurred if the risk event takes place. The Risk Impact Rating scale in Table 4 has been developed to assist with quantifying the impact.

The measurement of the consequences that do not have a natural monetary value, for example, reputation loss, need to be determined. Reputation loss, for instance, can be measured in loss of market value terms due to a reduction in share price. The main purpose of placing a value on the consequence is to get a feel for the magnitude of risk and its priority.

Table 4: Consequence and Impact Ratings

Impact Rating	Level of Consequence	Description	Financial Impact	Legal	OH&S	Licence to Operate	Reputation
5	**Catastrophic**	Severely impairs the ability of the company to operate as a going concern	>$100m	Major litigation, no settlement, maximum fine imposed on company, large fine imposed on individuals and potential imprisonment	Multiple fatalities, large numbers of severe injuries	Will result in withdrawal of mining leases/licences; prohibition to operate; delisting from ASX	Widespread negative community sentiment; withdrawal of public and/or political support for continued operations
4	**Major**	Will have a significant impact on the operations of the company; will likely require market disclosure	$10m - $100m	Significant litigation, settlement unlikely, medium fine imposed on company, small fine imposed on individuals is possible	Death, extensive injuries, significant hospitalisation	Warnings from statutory bodies; fines and/or court action to seek remedies for breach	Damage to reputation causing delays or interruptions to existing or planned projects
3	**Moderate**	Requires CEO and ELG intervention to manage and resolve; may consume considerable resources to manage taking attention from day-to-day operations' notification to Board	$500k - $10m	Minor litigation, settlement possible, small fine imposed on company, no fine imposed on individuals	Long term medical treatment required, however no fatalities, some hospitalisation	Infringement notices issued	Local or community issue involving political involvement (e.g. formal ministerial correspondence) or inconveniencing operations
2	**Minor**	Requires Executive-level intervention to manage and resolve; notification to CEO	$10k - $500k	Possible litigation, settlement likely, fine imposed on company is possible but unlikely, no fine imposed on individuals	Small number of injuries, first aid or outpatient hospital treatment	Regulatory bodies notified of breach	Adverse media coverage with short term damage to reputation

Impact Rating	Level of Consequence	Description	Financial Impact	Legal	OH&S	Licence to Operate	Reputation
1	**Insignificant**	Is expected and can be managed through already-approved operations	<$10k	No litigation, claims covered by workers compensation and less than deductible for property damage, no fine imposed on company or individuals	Incident not requiring medical intervention	Managed through internal operations	Minor effects on external relations

The Inherent Risk Rating equals the sum of the Likelihood Rating and the Impact Rating.

The Inherent Risk Rating is then classified as per Table 5.

Table 5: Risk Rating

Risk Rating	Classification	Required Action
Greater than 8	Extreme	Advise Board and monitoring required by ARMC
7 to 8	High	Advise Board and monitoring required by ARMC
5 to 6	Moderate	Regular monitoring required Executive Management
Below 6	Low	General monitoring required by staff in functional area

The risk matrix in Table 6 can be used to combine LIKELIHOOD and CONSEQUENCE to obtain a risk score.

Table 6: Risk Analysis Matrix for Determining Level of Risk

CONSEQUENCE					
Catastrophic	Low 1	Moderate 2	High 3	Extreme 4	Extreme 4
Major	Low 1	Moderate 2	Moderate 2	High 3	Extreme 4
Moderate	Low 1	Low 1	Moderate 2	Moderate 2	High 3
Minor	Low 1	Low 1	Low 1	Moderate 2	Moderate 2
Insignificant	Low 1	Low 1	Low 1	Low 1	Low 1
	Rare	**Unlikely**	**Possible**	**Likely**	**Almost Certain**

LIKELIHOOD

A realistic assessment is required as 'under' or 'over' optimism regarding either the Likelihood Rating or the Impact Rating will have a major impact on the approach to mitigation.

The above evaluation process gives management and directors some feel for the magnitude of the inherent risk in running the business and will assist:

- the Directors to understand the potential risk profile of the entity, i.e. the losses to which the business will be exposed if no mitigation is put in place or if mitigation strategies fail
- prioritising the risks to mitigate
- in determining a reasonable cost to allocate for the implementation and on-going maintenance of the mitigation strategies.

Any risk identified as having an Impact Rating of 5, irrespective of the Likelihood Rating, requires a mitigation strategy to be developed and monitored.

Tools and techniques for risk analysis can include:

- likelihood/consequence risk matrix
- hazard and operability studies (HAZOP)
- scenario analysis
- cost/benefit analysis (CBA)
- decision trees.

Velocity of Risk

While not yet discussed in the Australian Standard, an added element to risk analysis is an assessment of the velocity of risk, which can be defined as how quickly a risk area goes from the onset of the risk to the impact of the risk. The use of this rating recognises that traditional risk assessments which prioritise risk on likelihood and consequence can be outpaced by the speed at which risks can move throughout an organisation.

Table 7 sets out the ratings that can be incorporated into the Risk Register and inform the risk management process.

Table 7: Risk Velocity Ratings

Rating	Description	Elaboration
1	Advanced warning	Event can occur from the onset of the risk to the impact of the risk in more than a year
2	Moderate warning	Event can occur from the onset of the risk to the impact of the risk in 6 months to one year
3	Some warning	Event can occur from the onset of the risk to the impact of the risk in 1 to 6 months
4	Minimal warning	Event can occur from the onset of the risk to the impact of the risk in 7 to 30 days
5	No warning	Event can occur from the onset of the risk to the impact of the risk in 7 days or less

A risk that achieves a rating of 4 or 5, i.e. the onset of the risk to the impact of the risk ranges from less than 7 to 30 days or less, should be incorporated into crisis management plans. Risks that are rated as having a velocity of 1-3 can be dealt with in the normal course of risk management.

The velocity of risk rating is incorporated into the Risk Register and monitored for any changes that warrant an escalation of the management of the specific risk.

Step 4: Evaluate the Risks

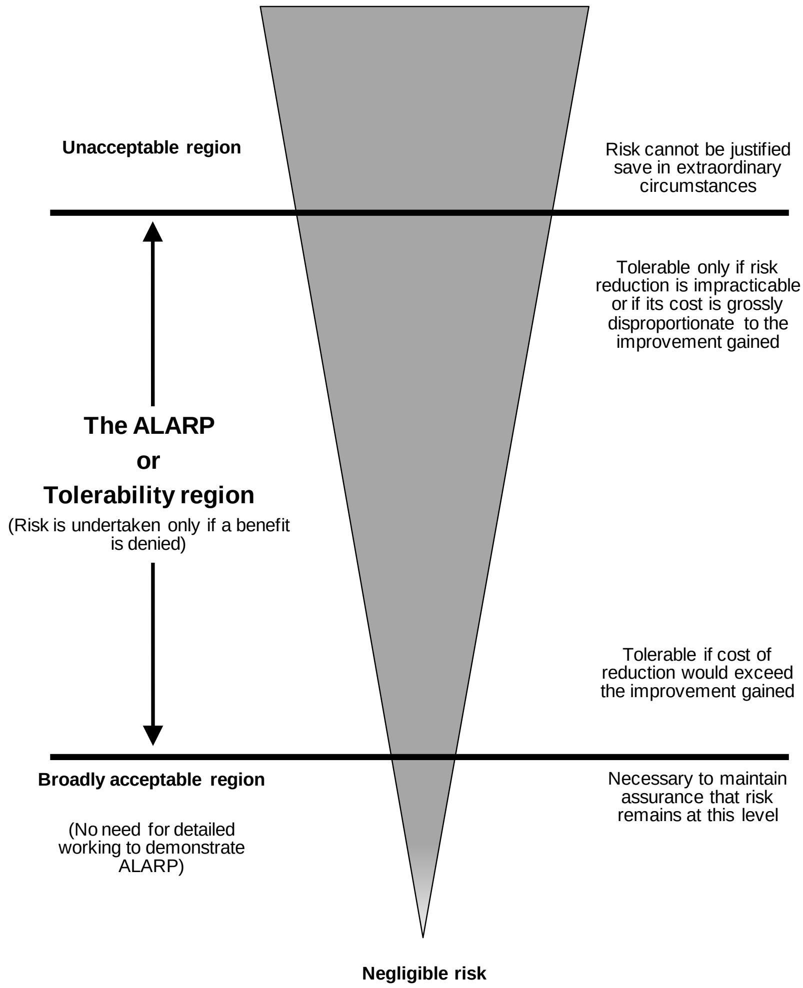
(References: AS/NZS ISO 31000:2009, s. 5.4.4; IEC/FDIS 31010:2009, s. 5.4)

'The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation' (AS/NZS ISO 31000:2009, p. 18).

Having identified and analysed the risk, the issue becomes how the risk is to be handled. Board, management and strategic priorities will generally determine how risks are prioritised for treatment. In doing so, the ALARP ('As Low As Reasonably Practicable') principle can be applied. The ALARP principle is used to determine how an organisation can best reduce its risk exposures to within tolerable levels.

ALARP is often used for risks that will have negative consequences, particularly those involving risks to people or the environment. For a risk to be ALARP, it must be possible 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 it would be possible to spend infinite time, effort and money attempting to reduce a risk so that it is negligible. Deciding whether a risk is ALARP can be challenging because it requires the Board and management to exercise judgment.

Figure 4: As Low As Reasonably Practicable (ALARP) Principle



Adapted from *IEC/FDIS 31010:2009*, p. 79

A cost/benefit analysis (CBA) is also tool often used in risk evaluation. The outcome of a CBA is only one of several considerations that go towards the judgment that a risk has been reduced to ALARP.

Other tools and techniques for risk evaluation include

- HAZOP
- root cause analysis
- Monte Carlo simulations.

Step 5: Treat the Risks

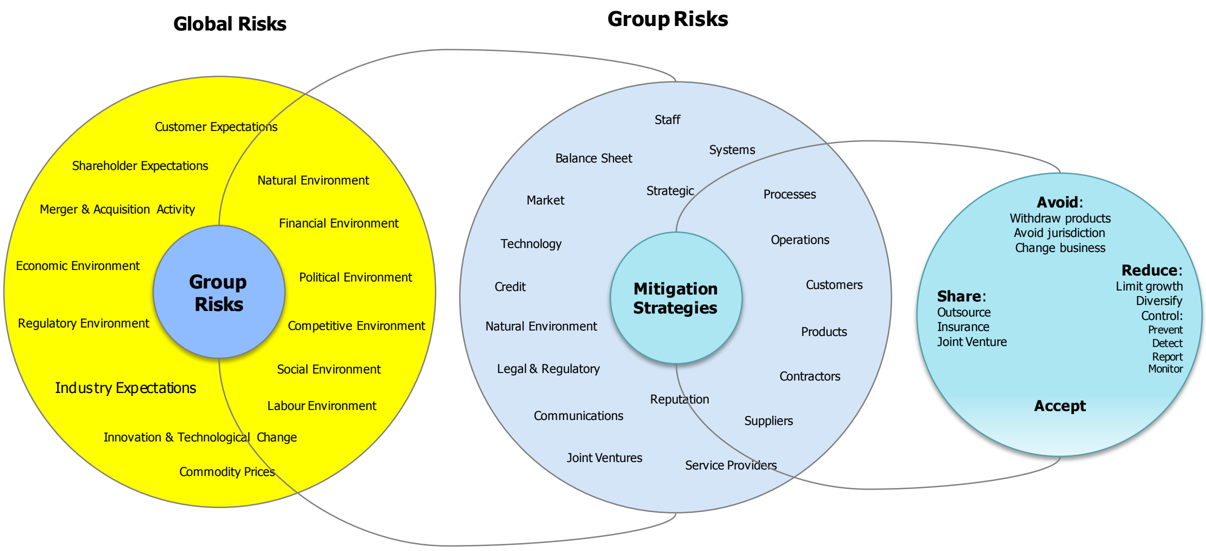
(References: AS/NZS ISO 31000:2009, s. 5.5; HB 436:2004, s. 8.2)

'Risk treatment involves selecting one or more options for modifying risks, and implementing those options' (AS/NZS ISO 31000:2009, p. 18).

Once the quantum of risks is assessed, the necessary responses to the risks can be determined.

As highlighted in Figure 5, responses to risk fall within the categories of risk avoidance, reduction, sharing and acceptance.

Figure 5: Mitigation Strategies



If the return likely to be achieved is not worth the likely cost of the risk, steps to avoid the risk need to be taken. This can be done by:

- withdrawing the specific products likely to cause the problems
- withdrawing from the problem jurisdiction
- changing the business completely.

None of these are steps to be taken lightly.

If the likely return is acceptable having regard for the risk, but that the total risk to be assumed is too large for Macarthur Coal's current resources, then the decision will be to share the risk with other parties.

The normal methods to share risks are to:

- outsource certain processes to a third party
- share the business project with joint venture parties
- insure the risk, either using normal causality insurance products or financial derivatives.

If a risk is shared, it does not mean that further risk mitigators, especially controls, are not necessary. It must be remembered that sharing current risks can create new risks, for example, credit risks or risks occasioned by lack of direct control of a process. If a risk is shared, a new risk assessment must be completed to identify, evaluate and, as necessary, mitigate the new risks assumed.

Risks may be accepted without further mitigation if they are either within management's tolerable residual risk limits at the inherent level, or else it is a risk which cannot be avoided, for example, it is an essential part of a larger process. In the case of the latter reason, adequate detective controls and stop-loss limits will need to be put in place and there should be a sign-off by the Board that the risk will be accepted for strategic reasons.

Risks can be reduced. This can be done by:

- limiting growth
- diversifying into other products or other markets
- establishing effective control mechanisms.

There are different forms of controls including:

- 'preventive controls' that reduce the likelihood of the risk event actually arising. They are proactive controls. Examples of preventive controls are separation of duties, proper authorisation, adequate documentation and physical control over assets.
- 'detective controls' that identify when a risk event has occurred and allow action plans to be initiated to restrict the quantum of any consequence. Examples of detective controls are reviews, analyses, variance analyses, reconciliations, physical inventories and audits.
- 'advisory controls' to ensure that the occurrence of the risk event is reported to management, the board, insurers, regulatory authorities, etc.
- 'restorative controls' to assist in repairing the damage to the business arising from the risk event and recovering from the risk event.

The exact level of mitigation put in place will depend on the level of perceived risk, the level of acceptable risk and the cost of implementing and maintaining the required mitigation strategies.

The mitigators in place need to be assessed. The criteria for the assessment of Mitigation Effectiveness is set out in Table 8.

Table 8: Risk Mitigation Effectiveness

Measure	Result	Characteristics
Poor	Risk will not be controlled	• No mitigators exist to manage risks or else are ineffective
Limited	No guarantee risk will be controlled	• Some informal risk management system, processes and procedures exist • Staff not fully aware of, nor understand mitigators to manage risk
Basic	Basic risks will be controlled most of the time	• Documentation of some risk management systems, processes and procedures exist and are reasonably understood by staff • Risk monitoring and management is informal Promotion of control environment is informal • Risk response action plans are informal
Good	Unexpected risk will be mitigated or detected in most circumstances	• Documentation of key risk management systems, processes and procedures exist and are understood by staff • Risk monitoring and management is occurring but is less structured Risk response action plans are identified and management ensures that controls are operating, although do not formally measure effectiveness of those controls • Management actively promotes a good control environment
Strong	Unexpected risk will be prevented	• Risk management systems, processes and procedures are formally documented, current and well understood by staff • Management ensures compliance with risk management policy and procedures • Management regularly monitors risk and risk triggers • Effectiveness of mitigators is formally monitored through use of predictive indicators • Management activity promotes a strong control environment

The next step involves the determination of the expected Residual Impact, that is, the Inherent Impact calculated earlier reduced by the effect of the mitigators which limit the quantum of the impact and / or the probability.

The methodology used to determine the Residual Risk is similar to that used to determine the Inherent Risk. The only difference is that the Likelihood Rating and Impact Rating are determined after consideration of the influence of controls in place to reduce the likelihood and / or consequence.

The Residual Risk is then classified as Extreme, High, Moderate or Low using the scale used for Inherent Risk.

The tolerance for the Residual Risk needs to be determined. Tolerance is the amount that can be foregone each year in respect of the risk. This amount must be aligned with the group risk appetite approved by the Board.

For controllable risk, the residual risk would normally be expected to be within tolerance where the effectiveness of the mitigation strategies was assessed as either 'Good' or 'Strong'.

If the Residual Risk is in excess of the tolerance for any risk, an Action Plan setting out the steps to be taken to reduce the risk to tolerable levels together with a reasonable time frame in which the Action Plan will be implemented must be prepared for management approval.

Step 6: Monitor and Review the Risks

(References: AS/NZS ISO 31000:2009, s. 5.6; HB 436:2004, s. 9.1)

Predictive Indicators should be identified to help monitor risks and the effectiveness of mitigators on an on-going basis.

A Predictive Indicator is a measurement indicator for monitoring the operation of mitigators against pre-set tolerances. In most cases, Predictive Indicators are Key Performance Indicators for the risk or its mitigation, for example, quality controls, expenses, etc. They could also be symptoms of poor performance, for example, customer complaints, negative media reports, poor staff morale, etc.

Predictive indicators can help management foresee problems which may lie ahead and assist in preventing losses or unfavourable outcomes through earlier management intervention. Whatever process is introduced, it needs to be able to indicate very early if a problem is arising and the process should be documented and applied consistently.

Change to Business and / or Business Environment

Whenever there are changes to the risk environment, a risk assessment needs to be undertaken to determine what responses are required, both immediately and in the future. If the changes are major, use the Risk Environment Change Model included in Table 9 below to identify the changes which require analysis and the areas which may be impacted.

Table 9: Risk Environment Change Model

	External			Internal	
	REGULATION	**MARKET**	**OTHER**	**ORGANISATION**	**OTHER**
FORCES OF CHANGE	New/proposed legislation: • International • Federal government • State government • Local government	Competitors	Shareholders	New strategies/ policies	Employee demands
	Court/tribunal decisions	Customers	Third party commentators: • Ratings agencies • Company analysts	Organisational changes: • M & A activity • Structure • Resourcing	Changes in assets or their ownership
	New/proposed regulatory action: • Enforceable • Voluntary	Suppliers: • Goods • Services • Capital	Community activist groups: • Environment • Consumer • Labour	New systems and processes	

Impacts of change	Strategies		People		Processes		Performance	
	Risks	Response	Risks	Response	Risks	Response	Risks	Response
Current								
Future								

Step 7: Communication and Consultation

(References: AS/NZS ISO 31000:2009, s. 5.2; HB 436:2004, s. 3.1; HB 327:2010)

'Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process' (AS/NZS ISO 31000:2009, p. 14).

As risks are interrelated, it is essential that communication and consultation with stakeholders across the Company takes place at each stage of the risk management process. A number of risks are the responsibility of one area while the mitigation is the responsibility of another area or function. For example, Marketing is accountable for the delivering the quantity and quality of coal to its customers in accordance with the contracts they have negotiated; Operations is responsible for producing the coal of the required quality and quantity at the required time.

Communication should address the risk itself and the process to manage it.

Effective internal and external communication is important to ensure that those responsible for implementing the risk management system and those with a vested interest understand the basis on which decisions are made and why particular actions are required.

Communication is a two-way process; it must flow upwards through management to the Board, and downwards to all staff from the Board.

Risk Registers

The information gathered at each stage of the Risk Management Process should be documented in the group Risk Registers.

In creating the Risk Register, the risk owners (i.e. the persons who are actually accountable for managing the risk and its consequences) can satisfy themselves that they have defined and properly addressed the real risk. It makes it easier to review the risks and ensure that they continue to be complete, relevant and accurate having regard for both internal and external changes.

Documentation of 'who does what and when', especially in respect of mitigators and monitoring programs and processes, ensures that the knowledge is not lost or degraded on loss of current staff.

Documentation of risks is the foundation for any meaningful verification process by senior management, the Board, ARMC or other Committees of the Board, internal and external auditors and regulatory authorities of the ongoing existence and relevance of, and compliance with, the risk management process.

Documentation may also be required evidence in insurance claims, court actions, etc.

Risk Registers should be dynamic documents; that is, as any risk, consequence, probability, mitigator or predictive indicator changes, the Register should be updated to reflect the current situation. Appendix 9.4 below contains a register template. Table 10 includes an overview of the information required to complete a register.

Table 10: Risk Register Overview

<table>
<tr><td>Risk ID #</td><td colspan="2">Unique identifier assigned to each risk in the register.</td></tr>
<tr><td>Category</td><td colspan="2">The category the risk fits into under the strategic risk categories identified:
• Financial
• Sales & Customers
• Rail & Port
• Project Evaluation
• Exploration
• Mining
• Strategy
• People
• Reputation</td></tr>
<tr><td>Generic Risk</td><td colspan="2">Based on the category, describe the risk in general terms, e.g. workforce shortage, debt, currency fluctuations</td></tr>
<tr><td>Specific Risk</td><td colspan="2">Describe the risk in detail</td></tr>
<tr><td>Triggers</td><td colspan="2">How can it happen?</td></tr>
<tr><td>Consequence</td><td colspan="2">Describe what will happen if the risk eventuates</td></tr>
<tr><td>Velocity of Risk</td><td colspan="2">Rates how quickly a risk area goes from the onset of the risk to the impact of the risk</td></tr>
<tr><td>Predictive Indicators</td><td colspan="2">The measurement indicator for monitoring the operation of mitigators against pre-set tolerances – the KPIs</td></tr>
<tr><td rowspan="4">Inherent Risk</td><td>Likelihood Rating</td><td>The chance of the risk/event happening if uncontrolled</td></tr>
<tr><td>Impact Rating</td><td>The impact of the risk before any control(s) has been implemented</td></tr>
<tr><td>Risk Rating</td><td>The inherent risk rating represents the level of risk/impact associated with a risk BEFORE the controls have been implemented to reduce the risk/impact</td></tr>
<tr><td>Risk Level</td><td>Colour coding based on level BEFORE control(s):
Extreme
High
Moderate
Low</td></tr>
<tr><td>Risk Owner</td><td colspan="2">Who will monitor this risk and its treatment, i.e. who is the risk owner? Risk ownership is a fundamental principle of risk management. Risk owners must remain fully aware of:
• Risk exposures (i.e. incidents)
• Pending risk assessments
• Outstanding reviews and actions
• Allocation of actions to be completed
• Breaches of risk tolerance</td></tr>
<tr><td rowspan="2">Risk Tolerance</td><td>Measure</td><td>How the risk tolerance is measured, e.g. % of spot sales to production</td></tr>
<tr><td>Metrics</td><td>The level set by the board/management for maximum tolerance of the risk, e.g. Maximum 10% spot sales</td></tr>
<tr><td>Preventative Controls</td><td colspan="2">The control(s) that reduce the likelihood of the risk event arising</td></tr>
</table>

<table>
<tr><td>Detective Controls</td><td colspan="2">The control(s) that identify when a risk event has occurred and to allow action plans to be initiated to restrict the quantum of any consequence</td></tr>
<tr><td>Effectiveness of Controls</td><td colspan="2">Describe how adequate current controls are using the categorisation set out in Table 6 of the Risk Management Methodology, i.e.:
• Poor
• Limited
• Basic
• Good
• Strong</td></tr>
<tr><td rowspan="4">Residual Risk</td><td>Likelihood Rating</td><td>The chance of the risk/event happening AFTER it is controlled</td></tr>
<tr><td>Impact Rating</td><td>The impact of the risk after the control(s) has been implemented</td></tr>
<tr><td>Risk Rating</td><td>The residual risk rating represents the level of risk/impact associated with a risk AFTER the controls have been implemented to reduce the risk/impact. It is expected that this score should be lower than the raw risk assessment</td></tr>
<tr><td>Risk Level</td><td>Colour coding based on level after control(s):
Extreme
High
Moderate
Low</td></tr>
<tr><td>Is Residual Risk Tolerable?</td><td colspan="2">Yes or no?</td></tr>
<tr><td>Action Plan for Improvement</td><td colspan="2">Describes how the chosen treatment options will be implemented</td></tr>
<tr><td>Related Corporate Strategy</td><td colspan="2">What corporate strategy or strategies does this risk relate to?</td></tr>
</table>

9.2 ASX PRINCIPLE 7 – RECOGNISE AND MANAGE RISK

Principle

Companies should establish a sound system of risk oversight and management and internal control.

Risk management is the culture, processes and structures that are directed towards taking advantage of potential opportunities while managing potential adverse effects.

A risk management system should be designed to:

identify, assess, monitor and manage risk

identify material changes to the company's risk profile.

This structure can enhance the environment for identifying and capitalising on opportunities to create value.

Recommendation 7.1

Companies should establish policies for the oversight and management of material business risks and disclose a summary of those policies.

Recommendation 7.2

The board should require management to design and implement the risk management and internal control system to manage the company's material business risks and report to it on whether those risks are being managed effectively. The board should disclose that management has reported to it as to the effectiveness of the company's management of its material business risks.

Recommendation 7.3

The board should disclose whether it has received assurance from the chief executive officer (or equivalent) and the chief financial officer (or equivalent) that the declaration provided in accordance with section 295A of the Corporations Act is founded on a sound system of risk management and internal control and that the system is operating effectively in all material respects in relation to financial reporting risks.

Recommendation 7.4

Companies should provide the information indicated in the Guide to reporting on Principle 7.

9.3 MAJOR POLICIES

Continuous Disclosure Policy

The Continuous Disclosure Policy requires all price sensitive information to be released to the market through a structured process complying with the ASX continuous disclosure rules and that third party briefings are only conducted by authorised personnel.

Delegation of Authority Policy

The Delegations Policy specifies the authority levels delegated to staff for committing Macarthur Coal's funds, the subsequent expenditure of those funds and asset disposals.

Segregation of Duties Policy

The Segregation of Duties Policy requires the splitting of responsibilities applicable to financial transactions and custody of assets to minimise the opportunity for fraud to be committed and / or errors to be overlooked.

Investment Policy Applicable To Short Term Investments

The Short Term Investments Policy is to ensure that liquidity is maintained to meet operational requirements, that adequate credit controls are maintained to minimise loss of capital and that only authorised investment products are used.

Foreign Exchange Hedging and Foreign Exchange Hedging Product Policies

The Foreign Exchange Policy specifies the foreign exchange hedging limits to minimise exposure to currency risk caused by foreign exchange rate volatility.

Interest Rate Hedging Policy

The Interest Rate Hedging Policy specifies the interest rate hedging limits to minimise exposure to interest rate risk caused by interest rate volatility when obtaining new debt.

Intercompany Internal Interest and Management Charges Policy

The Internal Interest and Management Charges Policy sets out the methodology for intra-group charges between Macarthur Coal and its controlled entities.

Environment Policy

The Environment Policy specifies the need for Macarthur Coal's operations to be carried out at all times in compliance with all environmental legislative requirements, adhering to all relevant business codes of practice and having due regard to acceptable environmental standards.

Human Resources Policy

The Human Resources Policy specifies the need for staff to carry out company operations in compliance with all legislative requirements, adhering to all relevant business codes of practice and having due regard to required ethical standards.

Fraud and Corruption and Whistleblower Policy

Macarthur Coal operates with a zero tolerance policy regarding fraud and corruption. The Fraud and Corruption and Whistleblower Policy recognises the need for Macarthur Coal to protect its revenue, property, information and other assets from any attempt by employees, contractors or members of the public to gain by deceit any financial or other benefit, and to provide a confidential and anonymous mechanism for reporting of potential or actual fraud and corruption.

Safety Policy

The Safety Policy requires management and staff to run Macarthur Coal's operations safely and efficiently at all times.

Share Trading Policy

The Share Trading Policy specifies the need for all trading in the company's securities by employees and directors to accord with Common Law, the Corporations Act and the ASX Listing Rules to prevent employees benefiting from information which has not been released to the financial market.

Shareholder Communication Policy

The Shareholder Communication Policy seeks to facilitate effective communication with existing and potential shareholders and make it easier for shareholders to participate at general meetings.

Treasury Policy

The Treasury Policy is Macarthur Coal's governing document for financial risks managed by the Commercial department

9.4 RISK REGISTER TEMPLATE

Internal confidential document removed for external publication of the Risk Management Policy.

9.5 CERTIFICATION PROCESS

Stakeholders	Roles & Responsibilities
Board	• The Board agrees the overall framework and process adopted to support certification • On an annual basis the Board will, on the advice of the ARMC, receive the certification provided by the CEO and the CFO • The certification received in relation to the year-end will then enable the Directors to sign the Directors' Declaration in accordance with the *Act* section 295(4)
Audit and Risk Management Committee	• The ARMC receives the certification from the CEO and CFO and makes any enquiries it deems necessary in relation to the certification or the process supporting it • Once satisfied, the ARMC recommends adoption of the certification to the Board
CEO and CFO	• The CEO and CFO review the evidence provided by management to support certification including the summary report, the results of any investigations carried out by the Internal Auditor and any statutory non-compliance reports provided by the Company Secretary and assurance reports provided by the CRO • Once satisfied that the requirements of section 295A of the Act and ASX Recommendation 7.3 have been met, the CEO and CFO sign the certificate to be provided to the ARMC
Company Secretary	• The Company Secretary reviews the summary report and if deemed necessary makes any further investigations principally through referral to the Internal Audit function. The Company Secretary also signs as reviewed the summary report • The Company Secretary is responsible for developing/updating the Certification Questionnaire (internal control questionnaire) and managing the process • The Company Secretary is responsible for ensuring the Certification Questionnaire is distributed and for collating the completed questionnaires. The summary report should be compiled by the Company Secretary and reviewed and signed-off by the CEO
Reviewer	• The reviewer reviews all designated Certification Questionnaires and obtains any necessary clarifications or additional information from the business unit manager who completed each Certification Questionnaire. If unable to satisfactorily resolve any issues the reviewer refers the matter to the Internal Audit function manager. Once satisfied with the results of any investigations the reviewer signs off the Certification Questionnaire
Business unit operator/manager	• Business unit managers complete designated Certification Questionnaires making any necessary enquiries or undertaking any tasks necessary to complete the required information