

Rio Tinto

February 2009
www.riotinto.com

Risk policy and standard

This document sets out Rio Tinto's standard approach to risk analysis and management, commonly referred to as the *Risk standard*. It provides a basic framework for Group companies to build upon, in order to comply with Rio Tinto's *Risk policy*.

Message from the finance director

Dear colleague

Rio Tinto is proud to be a leader in our chosen areas of business. Our continued success depends on our ability to understand the challenges of a changing world, and to respond effectively. We recognise that uncertainty offers significant opportunities for innovation, value creation and competitive advantage.

We also know that there are potential threats inherent in much of what we do, and we are committed to minimising these. This is especially the case where the threats are relevant to personal injury or environmental harm.

This *Risk policy and standard* booklet describes our chosen approach to risk management which ensures that we meet our own high standards at every level in the business. As Board Risk Sponsor, I am responsible for ensuring that we manage risk effectively across the entire Rio Tinto organisation, but I cannot do this alone.

I invite your support and commitment to implement this *Risk standard* in all aspects of your work. We each have a part to play in managing risk by enhancing opportunities and minimising threats, so that together we achieve Rio Tinto's full potential.



Guy Elliott

Contents

Risk policy	2
Risk standard	3
Introduction	3
Risk analysis and management process	5
Risk process initiation	6
Risk identification	7
Risk evaluation	7
Risk management	8
Risk reporting	9
Risk updates	9
Definitions for the purpose of this standard	10

Risk policy

Rio Tinto recognises that risk is an integral and unavoidable component of our business and is characterised by both threat and opportunity.

The Group fosters a risk-aware corporate culture in all decision making. Through skilled application of high quality, integrated risk analysis and management, our staff will exploit risk in order to enhance opportunities, reduce threats, and so sustain competitive advantage.

We are committed to managing all risk in a proactive and effective manner. This requires high quality risk analysis to inform the management decisions taken at all levels within the organisation.

To support this commitment, risk analysis is applied to all facets of the business by management at appropriate levels, following the principles set out in the *Risk standard*.

Risk standard

Introduction

Risk analysis and management is undertaken within Rio Tinto as a source of sustainable business benefits and competitive advantage. We recognise that managing threats and maximising opportunities will ensure that business objectives are met in the most effective way possible, leading to increased value for the business and its stakeholders.

In addition, Rio Tinto undertakes risk analysis and management to meet internal and external compliance requirements:

- **It is required to achieve compliance with the demands of international standards of corporate governance, including the Higgs Combined Code and Turnbull in the UK, the Sarbanes-Oxley Act in the US, ASX Guidelines in Australia, and the King Codes in South Africa.**
- **Rio Tinto can satisfy external auditors that risk analysis and management is applied consistently across all business units and the different disciplines.**
- **All project submissions to the Investment Committee must incorporate a risk analysis.**
- **Rio Tinto business units use risk analysis and management as tools for running the business, including the preparation of business plans, the management of internal projects and investments, and the maintenance of safe and secure operations.**

A common approach to risk analysis and management must be adopted across all areas of application, and this Standard sets out the minimum required framework for implementing the Risk policy. All Rio Tinto managed activities, projects and businesses are required to develop their own, locally designed approaches to risk analysis and management for maximum effectiveness, building upon this framework. Businesses should examine the adequacy of existing systems and activities and then augment what exists, if necessary, to conform with this Standard.

Many existing businesses will already conform to this Standard; but those that do not must comply within six months. Acquired businesses will have 12 months from the date of acquisition to conform. To assist with implementation, guidance notes have been issued to provide additional background and information. Further guidance will be issued in response to emerging issues.

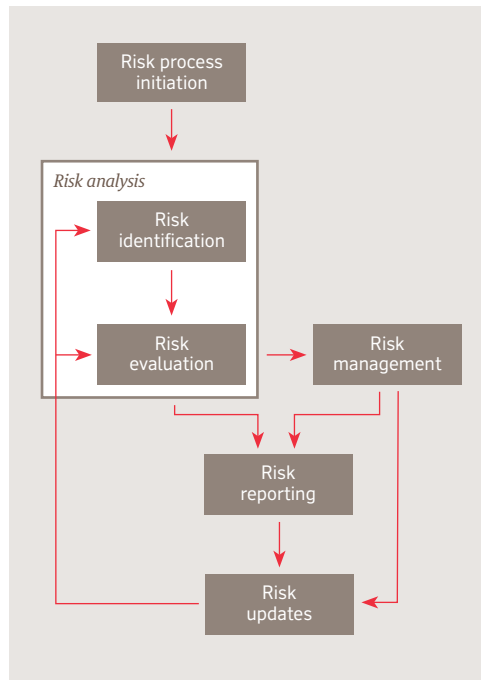
Valuable information on the design and implementation of effective risk analysis and management is contained on the Rio Tinto Risk Electronic Guidance and Information System (REGIS), located in the Rio Tinto intranet. Further advice and assistance is available from Rio Tinto's risk specialists in Technology and Innovation (T&I). This Standard is applicable to all Rio Tinto managed activities, projects and businesses. All Rio Tinto managed activities, projects and businesses must follow the minimum requirements laid out in this Standard when undertaking risk analysis and management.

Risk analysis and management process

Rio Tinto risk analysis and management must follow a uniform process to ensure consistency and high quality. The process includes six elements:

- 1 Risk process initiation
- 2 Risk identification
- 3 Risk evaluation
- 4 Risk management
- 5 Risk reporting
- 6 Risk updates

The relationship between these elements is shown in the diagram below.



Risk analysis and management process

Further details and guidance are available on REGIS.

Risk process initiation

A suitably qualified, competent person must be nominated to lead the risk analysis. The risk process initiation step must be led by this person, and must include the following tasks:

- Define the scope and context of the risk analysis, including explicit statement of what is in scope and out of scope
- Determine those objectives at risk, which are to be the subject of the risk analysis
- Define the methodology, tools and techniques to be used during the risk analysis
- Detail who will participate in the risk analysis, with their roles and responsibilities
- Define scales of likelihood and consequences to be used during the risk analysis, and define risk acceptance thresholds (see below)
- Describe the risk reporting and update cycles

The outputs from these tasks must be documented in a risk analysis plan.

Methods exist for defining likelihood and consequence scales (see REGIS for details), which apply to most Rio Tinto risk analyses.

The person leading the risk analysis must either:

- **Confirm applicability of the preferred method for the particular application before commencing the risk analysis, or**
- **Define and justify alternative scales to be used for a particular analysis.**

Clear and well defined risk acceptance thresholds are required in order to determine the level of risk that can be tolerated. Risk acceptance thresholds are based on defined scales for likelihood and consequences. Risks are then assessed and classified against the thresholds into one of the Rio Tinto Risk Management Classes I, II, III or IV, defined as follows:

- **Class I: Risks that are below the risk acceptance threshold and do not require active management**
- **Class II: Risks that lie on the risk acceptance threshold and require active monitoring**
- **Class III: Risks that exceed the risk acceptance threshold and require proactive management**
- **Class IV: Risks that significantly exceed the risk acceptance threshold and need urgent and immediate attention**

These four classifications apply equally to both threats and opportunities. Irrespective of the risk analysis process adopted, all risks identified and evaluated must be mapped to one of the Rio Tinto risk management classes.

Risk analysis and management process continued

Risk identification

The aim of risk identification is to expose and document all currently knowable risks which could affect achievement of the objectives. This includes both threats and opportunities, where a threat is a risk with a negative consequence, and an opportunity is a risk with a positive consequence.

Risks can be identified using a number of different tools and techniques. As a minimum, a facilitated risk identification workshop must be held with key stakeholders. In addition other techniques may be used at the discretion of the person leading the risk analysis. Detailed guidance on risk identification techniques is available from REGIS. Whatever risk identification technique is used, care must be taken to separate risks from their causes and effects.

Following initial risk identification, the possibility of risk aggregation must be considered, arising from interdependence or coincidence of identified risks. Aggregated risks must be recorded for special attention and subject to urgent evaluation.

Risks must be documented in a Risk register, at the level of detail required to support subsequent risk evaluation and risk management. Risk evaluation must not be performed during the risk identification process, in order to minimise bias.

Risk evaluation

The likelihood and consequences of each identified risk must be assessed using the predefined scales, and each risk must be classified and prioritised for further attention using the agreed risk acceptance thresholds. A 4x4 risk evaluation matrix is preferred, although 3x3 and 5x5 are permitted under specifically justified circumstances. Asymmetric risk evaluation matrices are not permitted. All risks must be classified according to the Rio Tinto Risk Management Classes.

The consequences arising from occurrence of risks can be either economic or non economic.

Economic consequences must be scaled when determining the level of risk acceptance (for example sensitivity to capital overrun will vary with project size). The economic consequences to be considered depend on the type of risk analysis, particularly whether it is for a capital investment project or for an ongoing operation. All Rio Tinto risk analyses must consider at least the following five types of economic consequence, all of which lead to a direct effect on NPV:

- **Capital expenditure**
- **Schedule**
- **Operating cost**
- **Production volumes**
- **Revenue**

Non economic consequences cannot be scaled. As a minimum, all Rio Tinto risk analyses must consider the following six types of non economic consequence:

- **Personnel safety**
- **Health impact**
- **Environmental impact**
- **Community impact**
- **Compliance impact**
- **Rio Tinto or business unit reputation**

Evaluation must be undertaken by internal Rio Tinto stakeholders with relevant experience and expertise, who have an overall knowledge of the area being analysed. This group must be able to judge the likelihood and consequences in the business and operational context, and consensus should be sought. The views of external experts should be obtained where this is considered necessary for a thorough evaluation of particular risks.

Special attention must be paid to any risks assessed as having very high negative consequence and very low likelihood. These include risks where consequences include multiple fatalities, a massive environmental incident, or a major plant or mine failure resulting in severe interruption to business. They also include aggregation risks arising from a number of related causes. Where such risks are identified, they must be noted in the Risk register as special cases, and treated immediately.

The results of the risk evaluation must be recorded in the Risk register.

In some cases it may be appropriate to use quantitative risk analysis methods to evaluate the effect of identified risks on achievement of objectives. Guidance on when and how to use these techniques is given in REGIS.

Risk management

Appropriate responses to each identified risk must be determined and implemented in order to optimise the level of risk exposure. Suitable risk responses must be developed by those with experience and expertise in the relevant area. Threats (risks with negative consequences) must be avoided, transferred or minimised. Opportunities (risks with positive consequences) must be exploited, shared or enhanced. Where such active risk responses are not possible, residual risks must be accepted with suitable levels of contingency. Guidance on risk response strategies is given in REGIS.

The cost effectiveness of each response must be determined before it is agreed or implemented. Agreed risk responses must be allocated to a single risk owner, and appropriate resources must be made available to ensure that responses are implemented effectively. The possibility of secondary risks arising from agreed responses must be considered. Progress on risk responses must be monitored against agreed milestones and targets. Where an agreed risk response is not

Risk analysis and management process continued

achieving the intended result, additional responses must be developed, perhaps with different risk owners.

Agreed risk responses must be recorded in the Risk register, together with their current status and progress towards their achievement.

Risk reporting

The results of the risk analysis process must be documented and reported to key stakeholders. All risk analyses must produce a Risk register to document identified risks, together with their evaluations and agreed responses. Other risk report formats may be developed for specific purposes. The Risk register must contain the following minimum information for each identified risk:

- **Unique reference number**
- **Date of last risk update**
- **Brief title of the risk**
- **Description of the risk**
- **Likelihood of occurrence**
- **Assessment of all types of consequences**
- **Risk level, determined from the likelihood and the highest consequence**
- **Risk responses (both candidate and agreed), together with their current status**
- **Risk owner**

The Risk register must retain information on all closed risks, to provide an audit trail and to assist in learning for future risk analyses.

Risk updates

All risk analyses must be updated in the light of progress, developments or operational improvements. The update must reflect the results of risk responses that have been implemented, and must also identify additional risks which have emerged since the last update. All risks in the Risk register should be re-examined to ensure that previous Class I and Class II risks have not developed a higher profile.

Definitions for the purpose of this standard

Effective risk analysis and management requires a shared understanding of key terminology. Rio Tinto has adopted a common risk language that is consistent with international standards. A glossary of other risk related terms is contained in REGIS.

Consequence

The outcome of a risk if it occurs. Threats have unfavourable consequences, and opportunities have favourable consequences. Consequences fall into two types: economic and non economic.

Inherent risk

The risk as originally identified before actions or controls have been implemented.

Likelihood

The chance that a particular risk will occur. This can be expressed as either a probability for a single event or condition, or a frequency of occurrence for repeat events.

Opportunity

A positive risk; an uncertain beneficial event or condition that if it occurs will result in favourable outcomes such as improved safety, saved time or cost, improved relations with communities and other stakeholders, or enhanced reputation.

Residual risk

The risk remaining after agreed actions and controls have been implemented.

Risk

An uncertain event or condition that if it occurs will affect achievement of one or more objectives.

Risk acceptance threshold

A measure of the level of risk exposure above which action must be taken to proactively manage threats and maximise opportunities, and below which risks may be accepted.

Risk analysis

The overall process of risk identification and risk evaluation.

Risk evaluation

The process of estimating the likelihood and consequences of identified risks, and comparing against a defined risk acceptance threshold.

Risk identification

A structured process to identify threats and opportunities.

Risk management

The process of taking appropriate decisions and implementing appropriate actions in response to known risks, based on the results of a risk analysis.

Threat

A negative risk; an uncertain adverse event or condition that if it occurs will result in unfavourable outcomes such as injury, damage to the environment, communities, stakeholder confidence, reputation, delays, or economic loss.

Rio Tinto plc

5 Aldermanbury Square
London EC2V 7HR
United Kingdom

T +44 (0)20 7781 2000

Rio Tinto Limited

120 Collins Street
Melbourne, Victoria 3000
Australia

T +61 (0)3 9283 3333

This booklet supersedes the *Risk analysis and management guidance* dated June 2005

© Rio Tinto plc and Rio Tinto Limited

Published August 2007

Revised 2009 and reprinted 2009/English