

Risk analysis and management guidance

June 2005
www.riotinto.com

This document provides guidance for Group managers on Rio Tinto's approach to risk analysis and management

Message from the chief executive

Dear Colleague

Risk analysis and management

Rio Tinto's internal processes mandate or encourage the use of risk analysis. External directives on corporate governance also allude to or specifically require it as an integral part of the way we conduct our business. Although the term is in common usage, its meaning is not always well understood. This *Risk analysis and management guidance* booklet has been produced to improve the definition of risk analysis within Rio Tinto, as well as providing both a minimum quality standard and some common terminology for use across the Group.

In future, any work done within Rio Tinto that purports to be risk analysis should comply with this guidance. Employees involved in risk analysis should familiarise themselves with its contents.

A handwritten signature in black ink, appearing to read 'Leigh Clifford'. The signature is fluid and cursive, with a large initial 'L' and 'C'.

Leigh Clifford

Contents

Introduction	2
Risk classification	3
Risk evaluation	4
Consequence types	4
Defining likelihood and consequence	5
Risk acceptance thresholds	6
High consequence low likelihood risks	6
Common risk language	7
Risk analysis process	8
Risk process initiation	8
Risk identification	9
Risk evaluation	10
Risk management	10
Risk reporting	11
Risk updates	12

Introduction

Rio Tinto recognises that all aspects of our business involve significant risk, including both threats (downside risks) and opportunities (upside risks). We are committed to managing all sources of risk in a proactive and effective manner through competent risk management. This requires high quality risk analysis to allow appropriate management decisions to be taken at all levels in the Group and business units. As a result, risk analysis will be applied to all facets of the business by management at all levels, following the principles set out in this *Risk analysis & management guidance*. Further detailed implementation advice is provided for businesses by the Rio Tinto Risk analysis & management portal (the “Risk portal”).

Risk analysis and management is primarily 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 our 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 USA, ASX Guidelines in Australia, and the King Reports 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

Risk analysis and management in Rio Tinto is applied broadly to all business activities. A common approach to risk analysis and management must be adopted across all areas of application, and this guidance provides minimum criteria to which all risk analyses will conform.

This *Risk analysis and management guidance* covers the following topics:

- 1 Risk classification
- 2 Risk evaluation
- 3 Common risk language
- 4 Risk analysis process

Each of these is discussed in the following sections. Detailed advice and guidance on implementation issues are provided on the Risk portal, which should be consulted prior to undertaking any particular risk analysis.

Risk classification

The decision on how best to manage a risk depends on an assessment of its significance. This requires a clear mechanism of classification which can be applied to any type of risk, including both downside threats and upside opportunities, and which is independent of the specific application.

The approach adopted within Rio Tinto defines a risk acceptance threshold based on the likelihood of occurrence and potential consequence(s), and then compares each identified risk against the threshold.

All identified risks are categorised into one of four classes, 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. Definition of the risk acceptance threshold is described in the following section. Various methods can be used to analyse the significance of risks, but whatever method is used must lead to classification of each identified risk into one of these four classes for reporting purposes.

Risk evaluation

Risks must be evaluated using a consistent set of criteria which is specifically defined for each risk analysis. Typically two factors are considered for each identified risk: the likelihood that the risk will occur, and the consequence(s) that would arise if it did occur. These two dimensions are also used to define the risk acceptance threshold against which individual risks are assessed.

This section addresses:

- 1 Consequence types
- 2 Defining likelihood and consequence
- 3 Risk acceptance thresholds
- 4 Low likelihood high consequence risks

Consequence types

Rio Tinto risk analyses address both threats and opportunities, where a threat is a risk with a negative consequence, and an opportunity is a risk with a positive consequence.

Rio Tinto risk analysis recognises that the consequences arising from occurrence of risks can be either economic or non economic. The principal difference is that non economic consequences cannot be scaled (for example a fatality would have the same impact to the business at all levels); whereas economic consequences must be scaled when determining the level of risk acceptance (for example sensitivity to capital over run will vary with project size). In addition, economic consequences can be either negative or positive.

Non economic consequences by contrast are usually negative.

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 will consider at least the following five types of economic consequence:

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

These five all lead to a direct effect on NPV. However, in addition, some risk analyses might require consideration of explicit consequences on NPV. Risk analyses of operations may also require more detailed definition of some consequences, for example maintenance cost as a component of operating costs, or ore mined/processed as details of production volumes.

As a minimum, all Rio Tinto risk analyses will consider the following six types of non economic consequence:

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

Defining likelihood and consequence

Standard methods exist for defining likelihood and consequence scales (see the Risk portal for details), which apply to most Rio Tinto risk analyses. The person leading the risk analysis must either:

- confirm applicability of the standard method for the particular application before commencing the risk analysis, or
- define and justify alternative scales to be used for a particular analysis

Typically both likelihood and consequence scales are defined with three, four or five points, usually using the same number of points for likelihood and for consequence (eg 3x3, 4x4 or 5x5). Four point scales are appropriate for most Rio Tinto risk analyses, since three point scales may not be sufficiently rigorous to allow adequate discrimination between different classes of risks, and five point scales may be overly complex. However 4x4 scales are not mandatory.

However many scale points are selected for a particular risk analysis, it is essential that their meanings are defined prior to commencing the analysis. An example four point scale for likelihood is presented in the table below, defining probability values for single risk events, and time based frequency values for repeated events. Other types of likelihood definitions may also be required (see the Risk portal for details). In some circumstances it may be appropriate to define likelihood as a combination of probability and exposure.

Example definitions of likelihood

Likelihood type	Class			
	Very unlikely	Unlikely	Probable	Highly likely
Probability	< x%	x% – y%	y% – z%	> z%
Frequency (time)	Less than once per p months	Once per p – q months	Once per q – r months	More than once per r months

Example definition scales for the main types of economic consequences are presented in the Risk portal, against which each identified risk can be assessed. Since risk analyses must address both threats and opportunities, it is necessary to define both downside and upside economic consequence scales. Threats have unfavourable economic consequences (increased capital expenditure or operating cost, delayed schedule or production, delayed or lost revenue); opportunities have favourable economic consequences.

Economic consequences are scaled to support risk analyses at different levels in the organisation, since risk acceptance thresholds for smaller projects or business units have lower absolute values than the thresholds for larger projects or business units.

Example definition scales for non economic consequences are also presented on the Risk portal, against which identified risks can be assessed. Definition of upper limits for unfavourable non economic consequences does not imply that they are acceptable to Rio Tinto, or

Risk evaluation continued

that a consequence at this level would be tolerated under any circumstances. It merely recognises that such levels of consequence are theoretically possible as upper limits.

Risk acceptance thresholds

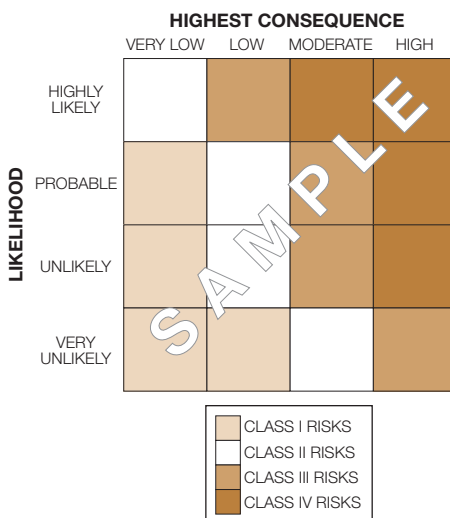
Clear and well defined risk acceptance thresholds are required in order to define the level of risk that can be tolerated. Risk acceptance thresholds are based on defined scales for likelihood and consequences. Risks are then assessed and classified using a risk determination matrix, using the same matrix for both threats and opportunities. An example 4x4 matrix is given here, where both likelihood and consequence are assessed against four point scales, and the risk acceptance threshold is shown in this diagram as the white zone (occupied by class II risks).

The example matrix has asymmetric zones which give more weight to consequence than to likelihood. The precise placement of zone boundaries reflects the risk acceptance threshold. Guidance on matrix definition is given on the Risk portal.

Where a risk has more than one type of consequence, its position in the matrix is determined by its highest scoring consequence.

The position of each risk in the matrix determines its classification into one of classes I, II, III or IV, as illustrated in the sample matrix. These classes indicate where the risk is positioned in relation to the risk acceptance threshold (see above).

Example risk determination matrix



High consequence low likelihood risks

Special attention needs to be paid to any risks assessed as having very high negative consequence and very low likelihood.

These may 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 may also include aggregation risks arising from a number of related risks.

Where such risks are identified, they should be noted in the Risk register as special cases, and treated separately from the standard risk analysis process, with further urgent evaluation. The Risk portal gives guidance on evaluation techniques for this type of risk.

Common risk language

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. Key definitions relevant to Rio Tinto risk analysis and management are reproduced below. A glossary of other risk related terms is contained in the Risk portal.

Risk

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

Threat

An uncertain adverse event or condition that if it occurs will result in unfavourable outcomes such as injury, damage to the environment, delay, or economic loss.

Opportunity

An uncertain beneficial event or condition that if it occurs will result in favourable outcomes such as improved safety, saved time or cost.

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.

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.

Risk analysis

The overall process of risk identification and risk evaluation.

Risk identification

A structured process to identify threats and opportunities.

Risk evaluation

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

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 management

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

Inherent risk

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

Residual risk

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

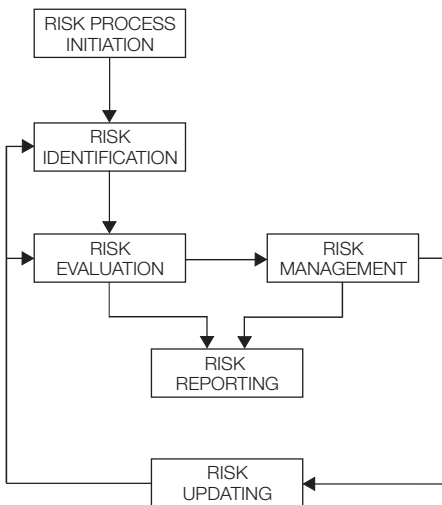
Risk analysis process

Effective risk management depends on competent risk analysis. Rio Tinto risk analysis and management follows a uniform process to ensure consistency and high quality.

This guidance presents a summary of the process, giving minimum criteria to which all risk analyses adhere. 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 below.



Further details and guidance are available on the Risk portal.

Risk process initiation

The risk analysis process is initiated by 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
- Describe the risk reporting and update cycle

Where necessary, inputs from appropriate stakeholders should be sought, and consensus achieved before proceeding with the risk analysis. The outputs from these tasks should be documented in a risk analysis plan. As a minimum this is based on a standard template, though a more detailed document may be produced where required.

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.

Risks can be identified using a number of different tools and techniques, including:

- Workshop/brainstorm
- Interviews (individual or group)
- Delphi panel (experts)
- Questionnaires
- Prompt lists and checklists
- Post-project review analysis
- SWOT analysis (Strengths, Weaknesses, Opportunities, Threats)
- Assumptions analysis

As a minimum, a facilitated risk identification workshop will 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 the Risk portal. Whatever risk identification technique is used, care must be taken to separate risks from their causes and effects.

Candidate risk responses may be identified during the risk identification stage, and these will be carried forward to the risk management step to be confirmed and allocated to an owner for action.

The facilitated workshop should include all key stakeholders who are able to contribute to identifying risks. The facilitator should be familiar with the scope of the risk

analysis and skilled in the risk process, and should be drawn from outside the team directly working on the area being analysed. A brainstorm process should be used, addressing each objective within the scope of the risk analysis. A hierarchical framework of potential risk sources (risk breakdown structure) may be used to ensure that different types of risk are considered. The facilitator should ensure that all ideas are captured, and should also manage the group dynamics in order to maximise participation.

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

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

Risk analysis process continued

Risk evaluation

The likelihood and consequences of each identified risk are assessed using the predefined scales and the risk determination matrix. Each risk is classified and prioritised for further attention using the agreed risk acceptance thresholds.

Evaluation should be undertaken by 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 also be obtained where this is considered necessary for a thorough evaluation of particular risks.

The results of the risk evaluation are 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 on the Risk portal.

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.

Where candidate risk responses have been identified earlier in the risk process, these must be considered during the risk

management phase, and either confirmed or rejected.

Threats (risks with potential negative consequences) must be avoided, transferred or minimised if possible. Opportunities (risks with potential positive consequences) must be exploited, shared or enhanced if possible. 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 on the Risk portal.

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 can be implemented effectively. The possibility of secondary risks arising from agreed responses should be considered. Progress on risk responses should be monitored against agreed milestones and targets. Where an agreed risk response is not achieving the intended result, additional responses must be developed, perhaps with different risk owners.

Agreed risk responses are 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 will 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. Recommended report formats are detailed on the Risk portal.

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

Business units may decide to use a number of Risk registers, each covering a different discipline (eg safety, operations etc). Where this is the case, key risks from each lower level Risk register should be summarised into a high level Risk register of critical risks to the business unit.

Specific formats of risk reports at

different levels of detail may be developed for each risk analysis, depending on the risk information requirements of key stakeholders. The person leading the risk analysis must determine these requirements and ensure that they are met.

Risk analysis should be an agenda item for routine planning and progress meetings, and routine risk reports should be used to reflect and communicate the current level of risk exposure to teams.

Various software tools are available to support production of the Risk register and other risk reports. Selection of commercial risk software must be undertaken with care, avoiding complex systems wherever possible. Details of available software tools are contained on the Risk portal.

Risk analysis process continued

Risk updates

All risk analyses must be updated in the light of progress, developments or operational improvements. The update must also reflect the results of risk responses that have been implemented, and must also identify additional risks which have emerged since the last update.

For ongoing operations or for long duration projects, risk analyses should be updated periodically at the frequency defined during the risk process initiation step, and whenever a significant milestone is approached. For other risk analyses, the frequency of update depends on the rate of change, and an update should be performed whenever a major change occurs or is proposed.

This Guidance refers in several places to the Rio Tinto Risk analysis & management portal (the "Risk portal"). This can be accessed at:

**[http://portal.riotinto.org/
portal/communities/
community.asp?CommunityID=530](http://portal.riotinto.org/portal/communities/community.asp?CommunityID=530)**

RIO TINTO

Minerals and metals for the world



Rio Tinto plc

6 St James's Square
London SW1Y 4LD
UK

Phone: +44 (0)20 7930 2399
Fax: +44 (0)20 7930 3249

Rio Tinto Limited

55 Collins Street
Melbourne
Victoria 3001
Australia

Phone: +61 (0)3 9283 3333
Fax: +61 (0)3 9283 3707

Design consultants Tor Pettersen & Partners.
Printed in England by The Beacon Press using their *pureprint* technology.
© Rio Tinto plc and Rio Tinto Limited.
06 / 2005