RioTinto

RIS-B-001

<table>
<tr><td rowspan="4">Group
Standard</td><td colspan="4">Title: Risk Management Standard</td></tr>
<tr><td colspan="4">Function: Risk</td></tr>
<tr><td colspan="4">No. of Pages: 10</td></tr>
<tr><td>Approved :
July 2019</td><td>Effective:
July 2019</td><td>Supersedes: Risk Policy & Standard - February 2014</td><td>Auditable From:
July 2020</td></tr>
<tr><td colspan="2">Owner:
Head of Risk</td><td colspan="2">Approver:
Rio Tinto Executive Committee</td><td>Target Audience:
Rio Tinto leaders
Risk Community of Practice members</td></tr>
<tr><td colspan="5">Direct linkages to other relevant policies, standards, procedures or guidance notes:
• RIS-A-001 Risk Policy, 2019
• GOV-A-002 Group Delegation of Authorities ,2015
• PES-B-002 Project Evaluation Standard, 2019
• HSES standards, procedures and related guidance</td></tr>
<tr><td colspan="5">Document purpose:
• Outlines the scope, definitions, roles and business performance outcomes for risk management
• Outlines the risk analysis and management process requirements
• Outlines risk expectations for documenting, maintaining and communicating risk information
• Outlines assurance of risk management process and outcomes</td></tr>
</table>

Risk Management Standard

1. Scope

Rio Tinto's risk management framework sets out the organisational foundations for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation. A key element of this framework is Rio Tinto's Risk Management Standard. Together with the Group's Risk Policy, the standard outlines the expected outcomes from risk management, the roles and responsibilities associated with implementing risk analysis and management effectively, and the minimum requirements that must be met.

1.1. This standard applies to all managed businesses and functions in the Rio Tinto Group, and should be applied at all stages of the business and investment life cycle. In accordance with Group Joint Venture Procedure (2018), Rio Tinto seeks to bring a commensurate level of rigour and discipline to its Joint Ventures as it does to its wholly-owned assets, through engagement and influence subject to applicable laws.

1.2. This standard is to be read in conjunction with other Group standards and procedures that outline any specific risk requirements. The standard is the principal document to underpin the Rio Tinto Risk Management Framework and is consistent with industry standards such as COSO (2017) and ISO31000 (2018).

1.3. Given the wide range of circumstances in which risk-informed decisions are made, Rio Tinto has adopted an approach that gives leaders the mandate to implement the risk process in a flexible way as long as the minimum requirements defined in this standard are met.

2. Business performance outcomes

Effective management of risks to business objectives is a key performance area for all leaders. Effective risk management requires the following:

2.1. Identify and evaluate the risks that matter most in achieving business objectives, so resources can be prioritised in the most efficient and effective way.

2.2. Effectively communicate risk management information to decision makers across the Group, so Rio Tinto can respond at the right level of the organization.

2.3. Embed risk awareness into all decision making processes to support leaders in managing risks proactively and effectively to improve business performance by either creating or protecting value.

2.4. Clearly defined roles and responsibilities for risk management.

3. Specific definitions used in this standard

3.1. Risk is the effect of uncertainty on objectives caused by variability and specific uncertain events. Risk can manifest as opportunities (upside) or threats (downside) and both require risk management (refer to Section 5.2c - Describe risks).

3.2. Risk Appetite: In Rio Tinto, 'risk appetite' is the term used to define the nature and extent of risks that the organisation is willing to take in order to meet the organisation's objectives, within the context in which it operates and in alignment with Rio Tinto's values and applicable laws. Section 5 of this standard outlines the requirements for confirming the risk appetite for the decision at hand, by applying Rio Tinto's Risk Evaluation Scheme within the Risk Analysis and Management process. For Health and safety risks the requirement is to manage risks to 'As Low As Reasonably Practicable' (ALARP) as defined in the HSEQ management system.

Depending on the type of risks, Group policies, standards and procedures also inform leaders of the organisation's appetite for taking specific risks. The appetite for taking risk is not of a static nature and may change over time depending on internal and external factors. It requires review by leadership as part of the organisation's core business processes and decision making authorities. Examples of these core business processes are: Group Strategy development; planning processes; investment evaluation and approvals; Group policies, standards and procedures approvals; and setting operational thresholds or delegation of authorities in areas such as treasury, commercial, corporate relations, health and safety, operations and capital management.

Furthermore, the Rio Tinto Risk Management Framework (refer Section 4.3 Table 2) sets out the responsibilities of risk management across all levels of the organisation, to enable an up-to-date view of its risk appetite and exposure (upside and downside).

3.3. Rio Tinto's Risk Evaluation Scheme operationalises the level of appetite for risk in Rio Tinto (financial and non-financial) to be applied in decision making and management across the organisation. The Rio Tinto Risk Evaluation Scheme in Appendix 1, consists of:

a. Scaled consequences describing levels of financial and non-financial impact;
b. Scaled likelihood classifications; and
c. A risk matrix which maps likelihood and consequences into four risk classes used to describe the materiality of risk exposure and to guide risk management response. Class III and IV risks exceed thresholds and require proactive management.

3.4. Risk tolerance is the range (or variability) in outcomes related to a specific objective, that an organisation or leader is willing to experience within the organisation's risk appetite.

3.5. Risk threshold is the limit of a risk exposure within the risk tolerance range which invokes proactive risk management in order to meet the planned objective.

3.6. Controls: A control is any measure (process, device, practice, or required action) that directly enables an opportunity, or prevents or mitigates a threat, to meet the objectives. Performance of the control is specifiable, measurable and verifiable (auditable).

3.7. Critical controls: A critical control is a control that is relied upon to enable an opportunity, or prevent or mitigates a threat, such that the absence or failure of the critical control would substantially impact the risk, despite the existence of other controls. In addition, controls with a high degree of interconnectivity that collectively strengthen enablement of key objectives, may also be classified as critical.

3.8. Material risks are Class III and Class IV risks.

4. Roles and responsibilities

4.1. The responsibility for identifying, evaluating and managing risks lies with all our employees and business leaders. The owners of risks and controls are responsible for:

a. Implementation and verification of performance of local controls and actions.

b. Risk information quality and currency.

4.2. In the context of the requirements set in this standard, the following roles apply:

a. Leader in the context of this standard is the owner of the objectives, the sponsor of the risk analysis outcomes and may also be the owner of some risks.

b. Risk owners are responsible for oversight of control and action owners, and the implementation and reporting of risk, control and action status.

c. Action and control owners are responsible for and have the requisite authority to implement actions and controls, including monitoring performance and effectiveness.

d. Risk coordinators are responsible for supporting their risk owners to maintain the currency and quality of risk information in the risk management information system and assist leaders in using risk to inform management decisions.

e. Risk business partners are responsible for supporting risk coordinators, leaders and risk owners in embedding active risk management into core business processes and decision making.

4.3. The role and responsibilities for risk management in Rio Tinto are described in Table 1.

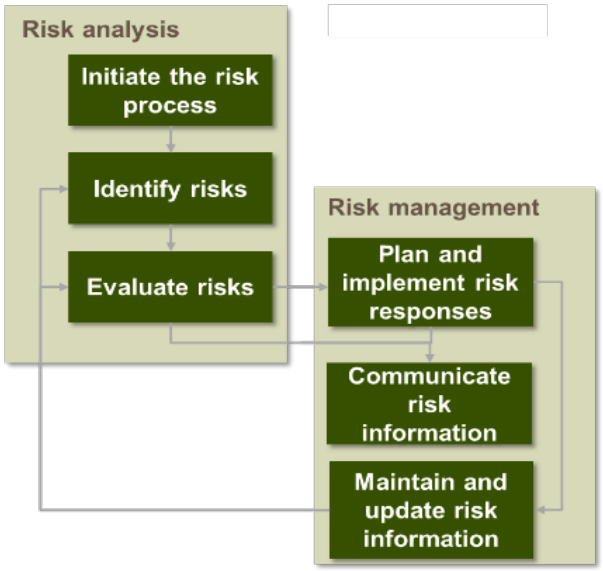
Table 1: Roles and responsibilities for risk management in Rio Tinto

Board Level	
Board	• Determines the nature and extent of risks that the organisation is willing to take in order to meet the organisation's strategic objectives. • Oversees risk management process and confirms that management's strategies are within the Board's risk appetite and tolerances.
Board Committees	• Monitors and reviews the maturity and effectiveness of our risk management framework. • Reviews management reports on the strategies and controls applied to any material business risks identified within the committees' scope.
Group Internal Audit	• Provides independent and objective assurance of the effectiveness of the risk management framework.
Group Level	
Executive Committee (delegations by CEO)	• Sets and reviews risk management strategies for risks to Group's business strategy, planning and investment decisions. • Defines the Group's risk tolerances around key business objectives and seeks Board endorsement of those tolerances. • Reviews the Group-level risks at least three times per year and approves material provided to the Board and its committees. • Approves new or revised Group-level controls (policies, standards and procedures) that support the management of material risks.
Risk Management Committee	• Monitors and reviews effectiveness of risk management framework across the Group's operations and functions on behalf of Executive Committee and the Board. • Provides oversight for the management of material Group-level risks and the associated management responses.
Risk function	• Coordinates and supports Group-level risk management activity and reporting. • Embeds risk management into core business processes, such as planning and capital allocation. • Builds risk management capability and a risk-aware culture throughout the Group.
Group's standard setters	• Develops, maintains and communicates Group-level controls, including policies, standards and procedures. • Verifies management's (Product Groups and Group functions) compliance to Group-level controls and the control effectiveness in managing risk.
Operational Level	
Senior leadership in Product Groups and Functions	• Manages material risks and critical controls within their business activities, escalating when appropriate. • Embeds risk analysis and management into their business strategy, planning and investment decisions. • Provides oversight of performance in their area of accountability through Risk, Assurance and Compliance forums.
Operational management	• Identifies, assesses and manages risks in areas in which management is accountable. • Executes line and functional management responsibilities for implementing and monitoring performance of actions and controls.
Risk Community of Practice	• Supports alignment, consistency and continuous improvement of risk management.

5. Minimum performance requirements

Rio Tinto has a single approved enterprise-wide risk management information system. At a minimum, all material risks must be documented and kept current in the enterprise system. A six-step Risk Analysis and Management Process is followed across the organisation. The six steps are: initiate the risk process, identify risks, evaluate risks, plan and implement responses, communicate, maintain and update risk information (outlined in Figure 1 below).

Figure 1: Risk Analysis and Management Process



5.1. Initiate the risk process

The initiation process follows a series of necessary steps, namely: define scope and purpose, set objectives, set risk tolerances and thresholds, create localised risk matrix, identify stakeholders and participants and nominate risk coordinator and facilitator.

a. Define scope and purpose: The leader defines the scope and purpose of risk information required for decision making. This includes documenting key assumptions underlying the risk analysis and how current controls and proposed actions should be reflected in the risk analysis outcomes.
b. Set objectives: The leader sets and prioritises the objectives that are requiring risk analysis and management.
c. Set risk tolerances and thresholds: The leader confirms the limits of variability or range of outcomes around each objective and sets risk thresholds that invokes management response.
d. Create localised risk matrix: The leader creates a localised risk matrix to be applied in the decision making and managing the set of objectives. This is done by mapping risk thresholds to the Rio Tinto Risk Evaluation Scheme, which operationalises the appetite for risk.
e. Identify stakeholders and participants: The leaders identify stakeholders and participants to contribute to the risk analysis. The stakeholders are those who may be impacted by the risks identified and may also contribute as participants. Participants should include those who can bring expertise, knowledge and diversity of thought.
f. Nominate risk coordinator: The leader defines the ongoing process for keeping risk information up to date and if required, nominates a risk coordinator to maintain and monitor the risk information and support facilitation of the risk process.

g. Engage facilitator: The facilitators of the process should be separate from those who will contribute to the content, remaining neutral and maintaining consistent application of the risk analysis process and inclusive participation.

5.2. Identify risks

The risk identification process follows a series of necessary steps: determine identification approach, identify sources of uncertainty, describe risk, current controls and apply taxonomy.

a. Determine identification approach: The leader determines the approach to document all potential risks that could affect achievement of the objectives, identified by key stakeholders and participants (eg facilitated workshop, questionnaire or focus group).
b. Identify sources of uncertainty relevant to objectives, including events that may or may not occur, incorrect or invalid assumptions and incomplete information.
c. Describe risk: The description of specific risk event (a risk statement) should distinguish between the risk (what might happen), the cause or source of the uncertainty (why it might happen) and the objective(s) that would be impacted if the risk occurred (consequence). By definition, a risk must impact on achieving objectives to be a risk, that is, not all uncertainties are risks. Furthermore, a risk is not the same as a problem or a constraint as they are certainties.
d. Document the current controls in place and operating, to inform the next steps in risk analysis process.
e. Apply risk taxonomy: The risk management information system contains a group-wide risk taxonomy to classify risks for profiling and data analytics. The taxonomy is applied to all risks.

5.3. Evaluate risks

The risk evaluation process follows a series of necessary steps: determine evaluation approach, assess effectiveness of current controls, evaluate risks and assign risk class and prioritise risk and determine management response.

a. Determine evaluation approach: The leader selects participants in the evaluation process who have sufficient expertise to determine the credible scenarios for the risks and the application of analysis techniques that minimise bias. A range of methods can be used to evaluate risks, but they must be able to be mapped back to the Rio Tinto Risk Evaluation Scheme.
b. Assess effectiveness of current controls: The evaluation participants assess the effectiveness of the overall portfolio of controls at the risk level using the Rio Tinto Control Effectiveness Scheme (Group Internal Audit Procedure, 2018) and document the rationale for the effectiveness rating.
c. Evaluate risks and assign risk class: Taking current controls into account, evaluate the level of consequences that could occur and the likelihood of the highest consequence, in order to assign the risk class (using 'localised' risk matrix per Section 5.1d). This 'evaluation rationale' is documented in the risk information management system.
d. Prioritise risks and determine management response: The leader uses the evaluated risk class to decide and prioritise which risks can be actively maintained and which require additional actions to be planned.

5.4. Plan and implement risk responses (actions and controls)

The process for planning and implementing actions and controls to manage risk exposure, follows a series of necessary steps: assign risk owners to risks, assign actions to risks, validate actions, assign action and control owners.

a. Assign risk owners to each risk: The assigned risk owner needs to have the requisite level of authority to manage the risk. In the context of non-managed operations, risk owners should be those persons in Rio Tinto best placed to influence the operator's management of the risk.
b. Assign actions to risks: Risk owners are required to assign actions to proactively manage all Class III and Class IV risks. These actions may improve current controls, create new controls or otherwise change the risk exposure. Where actions do not change the risk class to below risk threshold, active monitoring of the effectiveness of critical controls is required to manage the risk.
c. Validate actions: Risk owners will seek support from subject matter experts to validate actions, taking into consideration any other standards, local legal requirements or potential secondary risks that may arise. Risk owners document the rationale for why an action is appropriate and effective, given the nature of the risk.
d. Assign action and control owners: Risk owners assign action and control owners who are responsible for and have the requisite authority, to implement and monitor performance and effectiveness of actions and controls. All actions and controls require assignment of owners, due date for action implementation and review date for implemented controls.

5.5. Communicate risk information

Effective communication of risk information to decision makers and risk owners across the Group enables response at the right level of the organisation to achieve business objectives. Key considerations in effective communication of risk information includes the frequency, format and audience; clear articulation of risk, controls and action status to inform decision making; and escalation or delegation of risk ownership as required.

a. Determine the audience, format and frequency for risk communication, based on the materiality of risks and how quickly the risk exposure changes. Any assumptions made in presenting the risk information should be clear to decision makers.
b. Embed risk analysis into all decision making processes: Communication of risk information should clearly articulate what could change the risk exposure, control effectiveness or action status, and what intervention may be required to assist leaders in allocating resources in support of objectives and decision making.
c. Escalate or delegate risk ownership as required to enable risks to be managed and communicated at the most suitable level within the organisation. In any escalation or delegation, the handover must be properly managed to make sure the risk continues to receive the requisite level of attention. This includes the new risk owner accepting responsibility.

5.6. Maintain and update risk information

Maintaining and updating risk information includes monitoring the overall status and effectiveness of the portfolio of controls and actions and communicating changes in risk

exposure to appropriate stakeholders and management teams. At a minimum, two types of management review are required.

a. Review and update risk, control and action status: The leader, supported by their risk coordinator, updates risk analyses periodically to reflect changes in risk, control and action status in consultation with risk owners and subject matter experts. At a minimum of three times a year, review and update of Class III risks with moderate and above consequences and all Class IV risks is required. All other risks require at least an annual review.
b. Review and validate risk thresholds and overall risk profile: The leader, supported by a competent risk facilitator (endorsed by the Risk Business Partner), reviews and validates (1) risk thresholds against the business objectives (and any change to risk appetite) and (2) changes to risk exposure and control effectiveness for all risks. At a minimum, this review is required to ensure risk informs business strategy, annual planning and investment stage gates.

6. Assurance of this standard

The following outlines the lines of assurance to support effective implementation of risk management throughout the organisation.

6.1. First line assurance for this standard is through the risk management processes in operations, functions and projects, with oversight by senior leadership teams through the Risk, Assurance and Compliance Forums, to ensure the material risks and controls are being managed effectively. Risk Business Partners provide support to leaders to meet the standard's minimum performance requirements outlined in Section 5.

6.2. Second line assurance of this standard is led by the Group's standard setters to review the effectiveness of risk management including health checks, deep dives and other review activities. The Executive Committee or Risk Management Committee may also give direction to conduct assurance activities or programs relating to a specific risk or group of risks.

6.3. Third line assurance of this standard is conducted by Group Internal Audit to provide independent assurance that the risk management and internal controls are effective.

6.4. Additional risk-related assurance activities may be required by other Group standards.

7. Application

For more information on how to interpret and apply this standard, practice guidance and key contacts, you can refer to Rio Tinto's intranet.

Application for exceptions to this standard require approval from relevant Head of Function.