# Know Your Third Party Procedure

**GOV-C-006**

| **Group:** | **Function:** | **No. of Pages:** |
|---|---|---|
| Procedure | Rio Tinto Ethics & Compliance | 14 |
| **Effective:** | **Supersedes:** | **Auditable from:** |
| 1 July 2021 | KYS procedure (COM-C-002)<br>KYC procedure | 1 July 2023 |
| **Owners:** | **Approved:** | **Approver:** |
| Chief Ethics & Compliance Officer | 24 May 2021 | Rio Tinto Executive Committee |

**Target audience:**
All Product Groups, Business Units, Group Functions and managed Operations/Projects

**Direct Linkages to other relevant Policies, Standard, Procedures or Guidance notes:**

- The way we work
- Business Integrity Standard and Procedure
- Competition Standard
- Sanctions Standard
- Export Controls Procedure
- Partner to Operate Investment Procedure
- Group Procurement Standard
- Joint Venture Policy and Procedure
- Risk Management Standard
- Tax Policy and Procedures Manual
- New Country Entry Procedure

**Document purpose:**

This Procedure defines the accountabilities, responsibilities and due diligence processes applicable for the acceptance and engagement of new and existing third parties.

# Table of Contents

# 1. Overview

## 1.1 Purpose

Third party risk management is an end to end responsibility. Our commitment to ethical business conduct and to maintain the trust and support of our stakeholders is key.

A significant part of our business involves working with third parties. Rio Tinto's Know Your Third Party procedure sets out the requirements and mandatory processes to ensure that we adequately assess the risks, including reputational, represented by third parties with whom we may engage, whether these risks relate to potential economic sanctions, export controls, bribery and corruption, money-laundering/counter terrorism financing, other economic crime risks, enforcement actions, or human rights issues.

Knowing who we are dealing with, how the third party operates and being able to demonstrate that we have taken appropriate actions to assess and, when needed, mitigate any relevant risks related to that party is essential for operating in today's environment.

## 1.2 Scope

Compliance with the procedure is mandatory for all managed operations within the Rio Tinto group and for our business partners (e.g. joint venture partners) where contractually agreed.

The scope of the Procedure covers business activities by the Rio Tinto Product Groups, Group Functions, Business Units and managed Operations/Projects who have the responsibility for ensuring due diligence based on the risk criteria set out in this procedure.

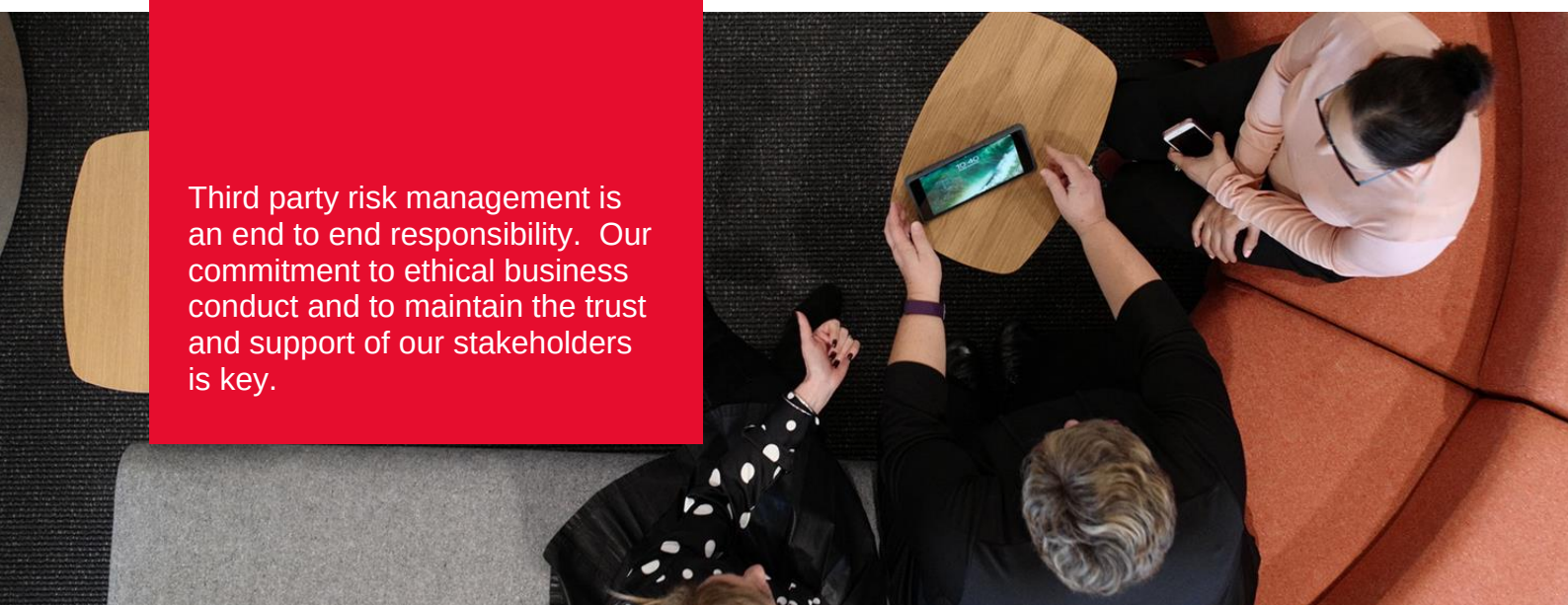
This procedure should be read in conjunction with *The way we work* and the Business Integrity Standard and Procedure. The Business Integrity Procedure further sets out the key principles and the common red flags to be alert to when dealing with third parties. All decisions and processes must align and comply with the applicable laws, regulations, and other relevant Rio Tinto policies, standards and procedures. If there is a conflict between this procedure and applicable laws or regulation, you must always comply with the most stringent requirement.

Rio Tinto's requirement is (a) to not make or accept payments in cash and (b) to not accept payments from/to third party payers/payees (not on-boarded as Rio Tinto third parties).

Ethics & Compliance will have the primary accountability for conducting the risk-based third party due diligence as set out in this procedure. No external service provider can be engaged to perform third party due diligence without consultation and prior endorsement in writing from the Chief Ethics & Compliance Officer.

Any applications for exceptions to the Procedure require approval in writing from the Chief Ethics & Compliance Officer.

Third party risk management is an end to end responsibility. Our commitment to ethical business conduct and to maintain the trust and support of our stakeholders is key.



### 1.3 Where should we go for help?

If you have any questions or are in any doubt whether a business transaction falls within the scope of this Procedure, please discuss the matter with your leader, the Third Party Due Diligence (TPDD) team, your regional Ethics & Compliance contact or send a question to *rt.duediligence@riotinto.com*.

### 1.4 What will happen should we fail to comply?

Compliance with the Procedure is mandatory and assured through monitoring. Failure to comply may have an adverse regulatory or reputational impact on Rio Tinto and may result in disciplinary action up to and including dismissal.

If you know or suspect a breach of this Procedure please raise your concern with your leader, a more senior manager, or your human Resources partner who in turn will report the matter to the Business Conduct Office. Alternatively, you can report your concern directly to the Business Conduct Office via *myVoice*, Rio Tinto's confidential reporting programme. No retaliatory action will be tolerated against anyone who has a reasonable basis for reporting an actual or suspected breach.

### 1.5 What is a third party?

A third party refers to an individual or an entity with which Rio Tinto and/or its managed operations enter into any legally binding agreement, commitment, or other business relationship. This includes but is not limited to customers, suppliers, contractors, organisations we partner or otherwise enter into an arrangement with (such as joint venture partners, acquisition and divestment targets), vessel, shipowners, charter parties, advisers (business, financial, legal and lobbyists), intermediaries, consultants, distributors, agents, recipients of financial or in-kind support including community organizations, and any other third party from whom we receive or make payment to.

Key third parties described in this document include:

- **New third party -** individual or entity that Rio Tinto seeks to engage with for the first time and/or is not registered in the Rio Tinto systems.
- **Existing third party –** active individual or entity where Rio Tinto will renew or extend an existing relationship in the Rio Tinto systems.
- **Inactive third party –** individual or entity which Rio Tinto has not transacted with in the last 2 years. When seeking to renew this relationship, this will be treated as a new third party.
- **Third party on internal watch list –** individual or entity that as a guidance, Rio Tinto will not enter into business or engage with, either directly or indirectly without written approval from the Chief Ethics & Compliance Officer or delegate. *This list* is maintained and reviewed periodically by the Third Party Due Diligence team; any additions or deletions to this list must be approved by the Third Party Due Diligence Lead.

### 1.6 Roles and responsibilities

The Product Groups, Business Units, Group Functions and Managed Operations/Projects have the ultimate responsibility to assess the third-party risk criteria set out in this procedure and to ensure that appropriate due diligence review is initiated and completed prior to entering into any legally binding agreement or other commitment, a business relationship or any other type of transaction with a third party.

The TPDD team is responsible for conducting a due diligence review established on the risk-based assessment and providing a risk-rated report with recommendations and where required, risk mitigation actions that are to be implemented by the business prior to engaging / entering into a commercial or legally binding commitment with the third party. In addition to ensuring risk mitigation actions arising from the due diligence review are implemented, the business is also responsible for ensuring other applicable counterparty verifications (such as credit approvals) are undertaken prior to engagement.

The regional Ethics & Compliance team will work with the Product Groups, Business Units, Group Functions and managed Operations/Projects to provide advice and agree on a plan to implement the actions and/or recommendations from the due diligence report. For certain proposed third party engagements the regional Ethics & Compliance team may undertake, either in parallel or following the issuance of the due diligence report, a compliance review/assessment in accordance with the recommendations and/or as required under the Business Integrity Standard and Procedure. In these circumstances, no engagement is to proceed until such a review/assessment has been completed satisfactorily as the outcome may impact the overall risk profile and/or mitigating actions.

Further details on roles and responsibilities are described under ***Appendix 2***.

## 2. Third Party Risk Assessment

Rio Tinto uses a risk-based approach to determine the appropriate level of due diligence review to be performed on a third party. This procedure sets out the risk criteria considerations, due diligence requirements and the overall risk rating methodology to ensure identified risks are adequately mitigated and managed. All third parties we seek to engage with require the identification, assessment, mitigation and monitoring of associated risks.

### 2.1 Third parties subject to this requirement

Third parties meeting the risk criteria under section 2.3 are subject to a due diligence review prior to entering into any agreement or commitment with Rio Tinto. This includes but is not limited to instances when:

- Seeking to engage a new third party, including in tenders for shortlisted third parties
- Entering into, extending or renewing of a contract or legally binding commitment
- Entering into a novation agreement where there is a transfer of the contractual obligations of one party to a third party or replacing a contractual obligation with another one
- Raising a sales order, purchase order or making a One-time vendor or manual payment to a third party
- Making a payment, financial or in-kind contribution to a third party
- Entering into a joint venture or other partnership with a third party
- Material change such as legal entity changes, country, location of bank account, etc. of an existing third party.

Due diligence review and requirements may also apply to other parties to the transaction, for instance, ship-to parties, consignees etc.

In addition, some parties may be providing services to Rio Tinto indirectly (e.g. known sub-contractors/sub-agents) or have no direct commercial or legal commitment or business relationship with Rio Tinto. Where performing high risk activities (see Section 2.3), they may require a third party due diligence review where appropriate. This assessment will be done in conjunction with the Ethics & Compliance team.

Non-contestable spend such as legally required tax/statutory payments to governmental authorities or agencies as well as payments to employees (e.g. expense reimbursements) and credit card transactions are not subject to this procedure.

Payments linked to existing contractual agreements related to dividends[1], royalties and settlement amounts arising from disputes/litigation with external third parties are considered in-scope.

The following risk-based considerations must be implemented to manage the third party risks:


[1] This excludes shareholder dividends

### 2.2 Level of due diligence review

It is the responsibility of the business to do the initial assessment and to initiate the due diligence request.

**Baseline screening:**

At a minimum, all third parties including other parties to the transaction, must go through baseline screening, which includes screening of the third party entity/individual/vessel against:

- sanctioned countries list (***Appendix 4***)
- applicable sanctions lists (per the Sanctions Standard)
- internal watch list (***Appendix 5***)
- regulatory enforcement lists

It is Rio Tinto's policy to not engage in any direct or indirect transactions involving sanctioned countries or sanctioned parties (together, "sanctions targets"). This includes transactions involving goods originating from or going to sanctioned countries (e.g. aluminium destined to Iran). For further definitions and details clarifying each of these areas, please refer to the *Sanctions standard*.

If a third party is identified as a sanctions target this should be escalated to the TPDD team and Sanctions Subject Matter Expert for further review, guidance and advice as per the Sanctions Standard.

If a third party is on the internal watch list consultation with Ethics & Compliance is required for further risk assessment prior to any engagement.

**Third party due diligence:**

After baseline screening, based on the risk criteria set out in section 2.3 below, each third party must be assessed to determine if a further third party due diligence will be required as well as the level of due diligence and monitoring that will be applied.

### 2.3 Third Party Risk Assessment – Risk Criteria

If a third party meets one or more of the following risk criteria, a due diligence must be initiated:

1. **Activity:** Nature of the third party activity and the business relationship with Rio Tinto, level of government interaction involved, the regulatory environment and the nature of the goods being purchased or sold and/or services rendered. (***Appendix 3***)
2. **Country:** Country in which the third party will be operating in, including the country of registration/incorporation, where the third party will be rendering services, sourcing goods from and/or delivering goods to (including end destination of the product) and country where the bank account is held and/or payment is being made to/received from. (***Appendix 4***)
3. **Value:** The total monetary spend value to determine materiality of the engagement or transaction as per below criteria.

Application of the risk criteria in determine whether a due diligence is required is dependent on the type of third party as outlined in the table below.

### Risk Criteria Evaluation to determine due diligence requirements

**At a minimum, irrespective of the steps set out below, all third parties including other parties to the transaction, must go through baseline screening.**

| Applicable to | Process | Third Party Risk Assessment | Action |
|---|---|---|---|
| New/Existing | Step 1 | 1. Is the third party performing one or more of the **high-risk activities** set out in ***Appendix 3***?<br>2. For sponsorships, donations or community support – is the annual aggregate spend or total commitment value expected to be USD 5,000 or above? | If **yes**, initiate due diligence request<br>If **no**, go to Step 2 |
| New/Existing | Step 2 | Is any of the following in a sanctioned or restricted country set out in ***Appendix 4*** (Country risk classification)?<br>**Country risk classification*** refers to the highest classification of:<br>• Registration/incorporation<br>• Payment made to or received from<br>• Bank account location<br>• Goods/services provided to or delivered<br>• Country of origin (if known) where goods are sourced | If **yes**, initiate due diligence request<br>If **no**, go to Step 3 |
| New/Existing | Step 3 | Is the country of payment or bank account different to the country where services are rendered or where the third party is registered? | If **yes**, initiate due diligence request<br>If **no for NEW**, go to Step 4<br>If **no for EXISTING**, go to Step 5 |
| New | Step 4 | Is the **total commitment value** or **expected annual aggregate value** by the individual business expected to be **equal to or exceed** USD 100,000? | If **yes**, initiate due diligence request<br>If **no**, no further action |
| Existing | Step 5 | Was this third party on-boarded within the calendar year and will current commitment increase the **annual aggregate value** to be **equal to or exceed** USD 100,000? | If **yes**, initiate due diligence request<br>If **no**, no further action |
| Additional Notes | • Where a Business Unit/Function wants to apply stricter risk criteria, guidance must be sought from the Ethics & Compliance team<br>• Due diligence is performed at third party entity level and further due diligence requirements will be triggered based on existing third party criteria.<br>• Once a new third party is on-boarded, the existing third party risk criteria for due diligence will apply when renewing or entering into a new commercial or legally binding commitment. | | |

# 3. Due Diligence process and risk rating

## 3.1 Third party identification, documentation and due diligence review request

If the third party meets the risk criteria set out in Section 2.3 and third party due diligence is required, the Requestor will initiate a due diligence request and include all information and supporting documentation as per *Appendix 7*. The requestor will have the primary responsibility to maintain the relationship with the third party throughout the due diligence process.

**Tender process** - in cases where there is a need to conduct due diligence at an earlier stage, e.g. pre-qualification or tender, this should be done for the short-listed bidders meeting the risk criteria of this procedure.

## 3.2 Third party due diligence report

### a) Third party due diligence review

Upon receipt of the due diligence request, the TPDD team will review the following to assess if the due diligence review can proceed:

- Third party details
- Supporting documentation
- Background information, as applicable
- Information on publicly available data sources

The TPDD team will then subsequently assess the third party based on the risk profile to identify any potential red flags and risks in relation to:

- Economic sanctions and denied parties lists
- Bribery and corruption
- Human rights including labour rights issues
- Money laundering and tax evasion
- Politicians or political party officials, or officers or employees of political parties and all candidates for political office, Politically Exposed Persons (“PEP”) and State-owned Enterprises (“SOE”)
- World Bank debarments
- Law enforcement or other regulatory actions
- Health, safety and environmental violations/issues
- Adverse media
- Other reputational concerns

Where red flags are identified, the TPDD team will analyse potential risks in the context of preserving Rio Tinto’s reputation and the intended business relationship or transaction with the third party and reach out to the Requestor for further information and/or documentation as required.

### b) Risk Rating

Once the due diligence review has been completed the TPDD team will summarize the results of the due diligence review in a due diligence report. The report will include:

a) Overall risk rating
b) Mitigating actions to be implemented
c) Overall recommendation, including whether a commitment with the third party can proceed

The overall risk rating attributed to a third party will be based on the results as follows:

| | |
|---|---|
| **LOW RISK** | No material risks identified which will prevent RT from entering into a legal commitment with the third party.<br>Product Groups, Business Units, Group Functions and managed Operations/Projects are accountable and responsible to implement any identified mitigating actions.<br>If actions cannot be completed or if you become aware of information which could elevate the risk profile you must consult with Ethics & Compliance and/or the relevant appointed Subject Matter Expert as soon as possible. |
| **MEDIUM RISK** | Risks identified which require proactive management and/or oversight by the Product Groups, Business Units, Group Functions and managed Operations/Projects but do not prevent RT from entering into a legally binding agreement or commitment with the third party.<br>The Business Units/Functions are accountable and responsible to monitor the relationship and conduct of the third party and implement any identified mitigating actions.<br>If actions cannot be completed or if you become aware of information which could elevate the risk profile you must consult with Ethics & Compliance and/or the relevant appointed Subject Matter Expert as soon as possible. |
| **HIGH RISK** | Significant risks identified which require proactive management and/or oversight by the Product Groups, Business Units, Group Functions and managed Operations/Projects.<br>The third party **cannot be engaged** until the mitigating actions have been implemented in consultation with the Ethics & Compliance team and the appointed Subject Matter Expert to see if any further escalation is required and approval in writing from the business area General Manager and the Chief Ethics & Compliance Officer must be obtained.<br>The business justification for the need of appointing or retaining the 'high risk' third party should be documented as part of the approval request.<br>The Third Party due diligence team will record all required risk mitigation actions identified in HIGH risk rated reports in a central tracking system.<br>The business will be responsible for ensuring mitigating actions are implemented and verified.<br>The Business Units/Functions are accountable and responsible to monitor the relationship and conduct of the third party. If you become aware of information which could elevate the risk profile you must consult with Ethics & Compliance and/or the relevant appointed Subject Matter Expert as soon as possible. |
| **VERY HIGH RISK** | Serious legal or reputational risks, red flags that cannot be overcome or sufficiently mitigated are identified and/or the third party refuses to provide or provides incomplete or inaccurate information or is on the Rio Tinto internal watch list.<br>Engagement with the third party **is prohibited** and/or steps must be taken to terminate if it is an existing third party. |
| **UNRATED** | Insufficient information is available to finalise the due diligence review on the third party.<br>Third party cannot be engaged until all required information to perform a due diligence is provided. |

c) **Due diligence report –** the due diligence report will be issued within the prevailing standard Service Level Agreement (SLA) of 10 working days, or sooner.

The actual time is dependent on the:

- Level of due diligence required on the third party
- Completeness of documentation and information provided
- Extent of data available on the due diligence system and data sources
- Translation requirements if information is not in English
- Number of potential findings and nature of identified issues
- Internal escalation/advice requirements to Subject Matter Experts

In certain instances, particularly where the nature of findings or risk posed to the business requires further independent due diligence review because of a lack of information from the third party or data sources, an external provider may be engaged to provide a specialised due diligence report. This may extend the timeline and likely incur costs to be borne by the Requestor.

Financial analysis and credit checks are not part of this scope of review. Please refer to Group Credit and Trade Solutions teams for further guidance on this.

For major capital projects and/or other projects which involve potential due diligence review on many third parties, this must be handled separately between the requestor and the TPDD team to agree on approach and turnaround time.

Due diligence reviews can only be expedited on an exception basis if there is a valid business urgency. Requestors must make every effort to initiate the review process sufficiently in advance to allow for the turnaround time to complete the review.

In cases where the business need qualifies for an expedited due diligence, a separate Service Level agreement will be established between the business and the Third Party Due Diligence lead.

## 4. Risk mitigation recommendations and actions

Upon completion of the due diligence review and issuance of report, the Product Groups, Business Units, Group Functions and managed Operations/Projects are required to:

- Review the report and underlying details
- Raise any additional potential issues or information they are aware of not identified in the due diligence report to the TPDD team
- Manage any communication with the third party after the due diligence review
- Ensure all identified mitigating actions are implemented in accordance with the recommendations in the due diligence report, in consultation with the Ethics & Compliance team and the relevant Subject Matter Expert, as applicable
- If identified mitigating actions cannot be implemented, this should be brought to the attention of the Ethics & Compliance team and the relevant Subject Matter expert
- Decide whether to establish, maintain or suspend a relationship with the third party
- Notify the TPDD team of all third parties not engaged at the end of the tender process via *rt.duediligence@riotinto.com* to ensure that only selected third parties receive ongoing monitoring.

Results of the third party due diligence review are confidential and may not be disclosed outside Rio Tinto.

# 5. Transacting and Monitoring

## 5.1 Transacting

A written agreement or equivalent document with the relevant third party needs to be place before entertaining any activity, including making or receiving any payment or other in-kind contribution. The agreement must have adequate Business Integrity representations based on standard clauses determined by the Senior Counsel – Anti-Bribery & Corruption and the agreement needs to be reviewed by Legal before execution.

Relevant mitigating actions as a result of the due diligence results must also be contractually represented, as necessary.

## 5.2 Monitoring

Third parties that have been engaged must be monitored on an ongoing basis in the entire duration of the business relationship.

The Product Group, Business Unit, Group Function or managed Operations/Project managing the relationship is responsible to ensure that all identified actions from the due diligence review are implemented. If any issues arise which deviate from the agreed commercial or business activity or there is a change in the activity or information obtained at the start of the process that results in potential red flags which change the risk level as set out in the risk criteria, they have the responsibility to communicate this to the TPDD team and the regional Ethics & Compliance contact as soon as known.

Once due diligence is completed, the third party will be subject to ongoing automated monitoring. The TPDD team will review the identified updates and inform the Product Group, Business Unit, Group Function and/or managed Operation/Project if there are any material changes to the initial findings and/or recommendations that may alter the risk classification of the third party.

The Ethics and Compliance Monitoring team are responsible for second line of defence monitoring and assurance.

## 5.3 Record retention

All records must be retained in accordance with Rio Tinto's Record Retention requirements.

## 6. Glossary and Appendixes

*Appendix 1 – Glossary*

*Appendix 2 – Roles & Responsibilities*

*Appendix 3 – High Risk Activities*

*Appendix 4 – Country Risk Scoring*

*Appendix 5 – Internal watch-list*

*Appendix 6 – Due diligence flowcharts*

*Appendix 7 – Due Diligence information requirements, questionnaires and forms*