

# Compliance guidance

October 2003  
[www.riotinto.com](http://www.riotinto.com)

This document provides programme guidance and guidelines for Group managers on implementing the Group's policies including those contained in *The way we work*, Rio Tinto's statement of business practice.

## Rio Tinto

Rio Tinto is a world leader in finding, mining and processing the earth's mineral resources. The Group's worldwide operations supply essential minerals and metals that help to meet global needs and contribute to improvements in living standards. Rio Tinto encourages strong local identities and has a devolved management philosophy, entrusting responsibility with accountability to the workplace.

In order to deliver superior returns to shareholders over time, Rio Tinto takes a long term and responsible approach to the Group's business. We concentrate on the development of first class orebodies into large, long life and efficient operations, capable of sustaining competitive advantage through business cycles.

Major products include aluminium, copper, diamonds, energy products (coal and uranium), gold, industrial minerals (borax, titanium dioxide, salt, talc and zircon), and iron ore. The Group's activities span the world but are strongly represented in Australia and North America with significant businesses in South America, Asia, Europe and southern Africa.

Wherever Rio Tinto operates, health and safety is our first priority. We seek to contribute to sustainable development. We work as closely as possible with our host countries and communities, respecting laws and customs. We minimise adverse effects and strive to improve every aspect of our performance. We employ local people at all levels and ensure fair and equitable transfer of benefits and enhancement of opportunities.

Our success as a business depends not only on our skills and the quality and diversity of the Group's assets, but also on our shared commitment to be a dependable global partner and good local neighbour.

# Introduction

A demonstrable commitment to compliance is one of the hallmarks of good corporate governance. Rio Tinto has made this commitment a cornerstone of its statement of business practice, *The way we work*, which states:

**Business integrity:  
We undertake Rio Tinto's businesses with integrity, honesty and fairness at all times, building from a foundation of compliance with local laws and regulations and international standards.**

Over the last decade there has been an accelerated change in the legal and regulatory landscape of those countries where the Group conducts business. Globalisation has further promoted this trend through the proliferation of laws and regulations that have an intended extraterritorial effect. Concurrently, developments in corporate governance have highlighted the need to expand existing control mechanisms to allow boards to identify and manage all risks.

Against this backdrop, Rio Tinto has determined that it can best meet its corporate governance obligations, and the Group can promote the commitment to compliance in *The way we work* by requiring all Group businesses to develop and implement their own formal compliance programmes.

The purpose of the following Compliance guidance is to provide a framework to enable each Group business to implement

and maintain a best practice compliance programme which should identify and manage risks associated with the non-compliance with laws, regulations, codes, standards, and Rio Tinto policies.

Management of these risks should principally be directed at preventing incidents of non-compliance. However, in cases where prevention is not effective, management will be expected to rectify or mitigate the causes and results of the incident and make changes to existing systems and practices.

The programmes should not be viewed as a 'box ticking' exercise. They are an essential and integral part of good corporate governance, designed to foster a culture of compliance consistent with the principles set out in *The way we work*.

# Background

## Hallmarks of best practice

The hallmarks of best practice compliance programmes are that they are effective, open and transparent and that they be seen as such. Accordingly, the programmes must be capable of being monitored and assessed, internally and externally, for effectiveness and modified as appropriate.

The following guidance prescribes a framework that follows the philosophy and logic of management systems, such as the ISO standards. One of the principal purposes in taking this approach is to maximise the legal protection the programmes should afford the Group. In most countries where the Group does business, the existence of an effective compliance programme will provide legal defences to Group companies themselves as well as to their management and boards in the event of an incident of non-compliance. The defence may be an absolute shield against liability or operate to reduce fines and penalties, depending on the circumstances.

However, to qualify for such benefits, those accountable for the programmes must be able to show that due diligence was exercised with respect to all aspects of their design, development, implementation and maintenance. A programmatic systems approach to compliance will better ensure that the Group and its individual businesses will be able to establish, at any particular point in time, that the programmes are effective. Such an approach will better position the Group to achieve the principal goal of the programmes, to prevent, and if

prevention is not possible, to detect and manage incidents of non-compliance.

A programme built upon the framework contained in this guidance will allow Rio Tinto to meet the requirements of the UK Combined Code and the applicable standards in other jurisdictions where we operate.

## Document structure

The guidance outlines the criteria for a systems based compliance programme. Supporting information, examples and suggestions are provided in the programme guidelines. The programme guidance and guidelines will also be available on the Group's intranet.

# Compliance programmes

## Rio Tinto's Compliance Guidance and Guidelines

Guidance for Group managers on implementing compliance programmes.

### Guidance

Corporate commitment and accountability	4
Identification of risk	4
Incident prevention	4
Investigations	6
Follow up	7
Certifications	7
Assessments and reviews	7
Reporting and record keeping	8
Continuous improvement	9

### Guidelines

Guideline 1: Corporate commitment and accountability	10
Guideline 2: Risk profiling	12
Guideline 3: Incident prevention – training	14
Guideline 4: Incident prevention – operating procedures	15
Guideline 5: Investigations	16
Guideline 6: Follow up	18
Guideline 7: Certifications	19
Guideline 8: Adherence assessments	19
Guideline 9: Reviews	21
Guideline 10: Reporting and record keeping	22
Guideline 11: Continuous improvement	25

# Guidance

## Corporate commitment and accountability

Commitment to the programme should originate in the first instance from the Group company board or its equivalent (referred to here and in the accompanying programme guidelines as the ‘board’). The chief executive officer (CEO) or managing director (MD) and senior management should also assume ownership.

As a minimum, corporate commitment should be demonstrated through the following:

- The board should adopt a policy setting out a clear statement of commitment to compliance and a brief description of how it will be carried out, and how it will be subject to ongoing review and improvement.
- The board should maintain primary accountability for the programme. However, it can delegate overall day-to-day management responsibility for the programme to one or more senior executives, ideally comprising a small committee (referred to in this guidance and the guidelines as the ‘committee’). Such individual(s) should have reporting responsibility to the board or the CEO/MD.
- The board should provide the individual(s) accountable for the programme with sufficient human and financial resources to ensure the programme’s effectiveness.
- Responsibility for compliance should be incorporated into job descriptions.
- The board should adopt processes and procedures to ensure that the programme becomes an integral part of day-to-day operations.

- The board should broadly publicise these actions throughout the business to ensure its visible and open commitment to the programme.

## Identification of risk

The identification of compliance risk must be systemic and ongoing.

Prior to fully implementing the programme, Group company boards should assure themselves that they and management are fully aware of those laws, regulations, policies, codes and standards which, if contravened, could give rise to a material impact on their own or Rio Tinto’s:

- financial condition;
- reputation; or
- ability to achieve its business objectives.

Each Group company should undertake a structured risk profiling exercise to identify, categorise and weigh the risks it faces in the conduct of its affairs unless its board is confident that all relevant and material risks have already been identified in a similar exercise.

Each Group company should put systems in place to ensure that risks are reviewed at an appropriate frequency and that its board and management are made aware of changes in the risk profile.

## Incident prevention

In order to prevent non-compliance, Group companies should have in place documented procedures and training modules designed to advise employees what to do in particular

situations. Standard Operating Procedures should have compliance requirements in built. Specifically, the actions, procedures and systems outlined below should be maintained at all times.

### **Training**

Compliance training should principally be focused on advising employees what to do in particular circumstances as opposed to teaching them the law. Training should be focused on the control of inappropriate conduct.

Rio Tinto has created the Rio Tinto Compliance Training Centre (Centre). Access to the Centre is available through the internet, either directly or through Group company intranets. All Group companies are expected to provide compliance training through the Centre as and when relevant content becomes available. In cases where the use of the Centre is impractical, exemption should be obtained from the head of Compliance and alternative training methods agreed upon.

Group companies will be responsible for setting most training parameters, however the following are minimum requirements:

- All salaried employees should be required to train on the core modules relating to:
  - the customised module on *The way we work*;
  - e-mail usage;
  - careful business communications;
  - US employees should be trained on preventing workplace harassment.
- Employees should be allowed no more

than four months to complete a module.

- A passing grade of 80 per cent should be required excepting the module that provides training on *The way we work*, where a grade of 100 per cent is recommended.
- There are multiple options available for the committee to track progress. It is recommended that Group companies track training completions only and the attainment of a passing grade, not failures.
- Employees should be required to re-train on the core modules once every two years.
- Although the system allows for individual registration, it is recommended that the Group company pre-register its employees. Specific compliance training, over and above the Web based modules, may use a variety of teaching methods and media, designed to express concepts in a language and format that the target audience understands.

### **Operating procedures and systems**

Adopting suitably designed operating procedures, computer system designs, forms and contract documents may also prevent incidents of non-compliance. Changes to systems and procedures should be progressed in accordance with Rio Tinto Safety Standard A2 – Change Management.

### **Complaint handling/*Speak-OUT* systems**

Each Group company should implement the Group's *Speak-OUT* programme. This is an independent, internal and confidential

## Guidance continued

complaint handling system designed to capture, analyse and investigate compliance failures identified by employees. Equivalent complaint management systems should be adopted for complaints received from external sources.

### Response plans

Group companies should assess the applicability of emergency response procedures in the context of managing compliance risk. In this regard, reference can be made to the Rio Tinto Disaster Management and Recovery Programme's model plan template, available from Group Risk Management.

### Proper delegation of authority

The programme must include mechanisms to identify personnel and positions that could give rise to compliance risk. Systems need to be put in place to ensure that substantial discretionary authority is not delegated to individuals who could have a propensity for misconduct.

Mitigating compliance risk may include employee screening and reference checking. Human resource staff and legal counsel should be consulted to ensure any processes or procedures do not breach local laws or regulations.

### Discipline

The programme should ensure that intentional or negligent acts that result in an incident of non-compliance will be subject to disciplinary action and that this is made

clear to all employees. One indication of an effective compliance programme is that discipline is evenly and fairly administered and that it be seen as such by employees.

### Investigations

Group companies should develop a process for the identification, classification and analysis of actual or suspected incidents of non-compliance. Material incidents must undergo root cause investigations, with appropriate remedial actions identified and implemented.

Investigations should be conducted unless:

- the incident was immaterial; or
- the Group company is satisfied that it knows what happened, why and that remedial action has been implemented.

If an investigation is warranted, it should be initiated as soon as practicable. The investigation should be focused on the root cause and in seeking to determine root cause, the investigation should focus on and differentiate between behavioural and systemic causes.

The investigation should result in a written report. In addition to the findings and conclusions of the investigating party, the report should set out any recommendations for follow up actions directed at rectifying or mitigating the cause or results of the incident, as well as recommendations directed at avoiding recurrence.

In the conduct of investigations, the use of legal counsel is vital to obtain various legal privileges. This is a complex area of

law and reference should be made to guideline 5 on page 16.

### **Follow up**

Any follow up actions required as a result of an investigation must be documented and tracked.

A report describing the actions undertaken should be prepared following completion of the follow up exercise. The report should clearly detail those actions that are ongoing.

The Group company should be able to assess the effectiveness of follow up actions, including modifications to the programme. Accordingly, any modifications should be accompanied by criteria to allow for the assessment of their future effectiveness.

### **Certifications**

The responsible executive(s) should provide the board with an annual certification that the programme is being adhered to and, where it is not, that the deficiency has been identified and steps are being taken to ensure adherence.

Until the provision of further guidance, certification should be given to the product group chief executive and the Rio Tinto board through the Internal Control Questionnaire.

The committee and board should give due consideration to other certifications that would assist in the management and maintenance of the programme.

### **Assessments and reviews**

Mechanisms must be in place that monitor adherence to, as well as the effectiveness and relevancy of the programme. For the purposes of this guidance and the associated guidelines, the term 'adherence assessment' or 'assessment' should apply to the exercises undertaken to ensure adherence to the programme. The term 'review' will be used to describe the exercises targeted at evaluating and ensuring the effectiveness and relevance of the programme.

### **Adherence assessments**

There is often a distinction made between monitoring adherence and assessing adherence. The former generally applies to an ongoing exercise. The latter usually refers to a formal review and analysis undertaken at periodic points in time. Group companies are required to assess their programme on a sufficiently frequent basis so as to ensure adherence throughout their business.

In conducting adherence assessments, Group companies should:

- Conduct the assessments on an annual basis;
- Ensure appropriate resources are assigned for the assessment process;
- Discuss, agree and record the scope and criteria for the assessment; and
- Provide a report on the assessment's findings, conclusions and recommendations.

## Guidance continued

Assessment reports should be issued to the committee, the Group company board, the product group chief executive, the head of Compliance and the Rio Tinto board or its designees.

### Programme reviews

On a periodic basis Group companies should undertake a comprehensive review of the programme for effectiveness and relevance, including an evaluation of programme performance against its objectives and other prescribed criteria. The review should include a prospective strategic analysis to determine changes in the law, changes in the business and business practices and resulting changes in the Group company's risk profile. It should also provide the committee with any recommendations for programme modification. Results of the review should be documented and be issued in the same way as the reports relating to adherence assessments.

### Reporting and record keeping

Group companies must be able to establish that they have exercised due diligence in making the programme transparently effective. Record keeping and reporting are crucial to attaining these ends and businesses should develop procedures and systems to ensure effective record keeping.

A report should be prepared with respect to the implementation and maintenance of the programme. Such reports will substantiate to regulators and other stakeholders that the programme is

effective and diligently operated.

Reports should be generated for the following activities:

- Risk profiling;
- Training;
- Incidents;
- Investigations;
- Follow up;
- Adherence assessments and reviews; and
- Continuous improvement.

Records should be maintained in regards to the following:

- Risk profiling:
  - when commissioned, by and to whom;
  - when completed;
  - when reported, by and to whom; and
  - how incorporated into programme design, when and by whom.
- Incident prevention; training:
  - introduced and when;
  - accountability;
  - who is being trained and in what areas;
  - training requirements, eg how long to complete courses; and
  - periodic reports on adherence to training requirements (between adherence assessments).
- Incident prevention; other measures, eg linking of Standard Operating Procedures in performance:
  - what and when implemented; and
  - accountabilities.
- Occurrence of incidents:
  - fact that an incident occurred;

- was reported, when, by and to whom;
- consequences of incident; and
- nature of initial response.
  
- Incident investigation:
  - commissioned, when, by and to whom; and
  - completed; and
  - report issued, when, by and to whom.
  
- Incident follow up:
  - work commissioned, when, by and to whom; and
  - work was completed; and
  - report issued, when, by and to whom.
  
- Certifications:
  - delivered.
  
- Adherence assessments and reviews:
  - work commissioned, when, by and to whom; and
  - work was completed; and
  - report issued, when, by and to whom.
  
- Agenda and minutes of compliance committee meetings.
  
- Continuous improvement:
  - decisions and actions taken to improve the effectiveness of the programme and its operation.

### **Continuous improvement**

Continuous improvement is an integral part of a best practice compliance programme. The commitment to continual improvement must be embedded into the programme.

# Guidelines

## Compliance programme guidelines

Further assistance in designing a suitable compliance programme for individual Group companies is available in the form of the following programme guidelines (see the Rio Tinto intranet for updates). Further advice and assistance is available from the head of Compliance whose contact details are:

Richard Pierce, head of Compliance  
Rio Tinto Services Inc.  
100 Mill Plain Road Suite 329  
Danbury, CT 06811  
Tel: +1 203 546 3551  
Fax: +1 203 546 3559

## GUIDELINE 1: Corporate commitment and accountability

A programme cannot be successful unless commitment is present and continuing at the highest levels of the organisation. To demonstrate commitment and ensure accountability for the programmes, it is recommended that each Group company undertake the following actions:

- The board should adopt a policy clearly stating its commitment to compliance and a brief description as to how the commitment will be carried out, and how it will be subject to ongoing review and improvement.

*Comment: Group companies have adopted Codes of Conduct. Such Codes may well contain the requisite policy, either in their current form or with minor amendment.*

- The board should maintain primary accountability for the programme. However, it may delegate overall day-to-day management responsibility for the programme to one or more senior executives. Such individual(s) should have reporting responsibility to the board (or its equivalent) or the CEO/MD.

*Comment: Although the board or its equivalent must maintain ultimate accountability for the programme, a senior executive(s) should be charged with overall responsibility for its design, development, implementation and maintenance.*

*The standards (including AS 3806) envision the possible utilisation of a full*

time compliance officer and attendant staff. It is recognised this may not be feasible. A management model that has been utilised with success is a committee comprising senior managers from varying disciplines that, in addition to their other duties, collectively assume and execute the accountability for the programme. The programme will interrelate with other departments and functions, eg HSE and Internal Audit. Most Group companies have systems/processes that provide for internal oversight of these functions. If the committee management model is adopted consideration should also be given to merging the oversight of these related functions. This should assist in managing the administrative burden associated with these activities.

The committee may delegate responsibility, which could result in certain departments taking primary responsibility for compliance in certain areas.

- The board should provide the committee with sufficient human and financial resources to ensure the programme's effectiveness.

*Comment: Inherent in the recommendation that responsibility for the programmes be vested in a senior executive(s) is the recognition that there could well be a tension between a desire to control costs and the need to direct sufficient resources to an effective compliance programme. The committee should have sufficient clout*

*to ensure that this tension is appropriately addressed and the goal of achieving compliance is attained.*

- Responsibility for compliance should be incorporated into job descriptions.

*Comment: Consideration should be given to making demonstrated commitment to compliance a performance parameter for compensation purposes, especially amongst management.*

- The board should institutionalise compliance through the adoption of processes and procedures with the goal of ensuring that the programme becomes an integral part of day-to-day operations.

*Comment: Commitment can be shown and established in very simple ways. As an example, matters relating to the programme should always be an agenda item for any meeting of the board, and its executive committee or its equivalent.*

- The board should broadly publicise its responsibilities and accountability throughout the business. There must not only be commitment, it must be visible.

## Guidelines continued

### GUIDELINE 2: Risk profiling

In assessing the need for, or in undertaking a risk profiling exercise, best practice requires that the programme focus on the types of risks the business engenders. Even if the committee elects not to commission a formal risk profiling exercise, there must be a concerted effort to identify the material legal, regulatory and business conduct risks confronting the business.

This guideline does not seek to provide a detailed methodology for the undertaking of such a risk profiling exercise. The head of Compliance can provide advice and assistance.

In the undertaking of a risk profiling exercise the following matrix can define all legal and regulatory risks faced by Group businesses (see below).

Board members should be confident that their perception of risk takes into account the categories appearing below.

There are numerous methodologies that can be utilised in conducting a risk profiling. One approach, common to ISO type management systems, is to first define, categorise and analyse the fact patterns associated with operations.

Another approach is to look at the business as a holistic process and undertake a SWOT analysis (strengths, weakness, opportunities, threats).

A third approach is to have legal counsel audit a select subset of the company's past activities. This is done through interviews and an analysis of records. This is the methodology utilised in the US when a company undertakes what

<b>Legislative and regulatory (civil and criminal)</b>	<b>Contractual</b>	<b>Common law or its civil code equivalent</b>
<b>A</b> Risk associated with non-compliance, including criminal prosecution and civil claims based on non-compliance brought by regulators or private parties	<b>B</b> Risk associated with defending or containing claims based on alleged breach of contract; including claims as to existence of unwritten contract	<b>C</b> Risk associated with defending or containing common law claims (eg negligence, libel, slander, trespass etc)
<b>D</b> Risk associated with a third party's non-compliance (as above) that puts Group assets, financial health or reputation at risk	<b>E</b> Risk associated with failing to invoke/enforce contractual rights	<b>F</b> Risk associated with failing to invoke/prosecute common law claims (as above) against third parties

is referred to as a Sentencing Guidelines Audit. Further information on Sentencing Guidelines can be found at [www.ussc.gov](http://www.ussc.gov)

Each of the methodologies described above have been utilised by Group companies in the past. There is no one correct way to perform a risk profiling. The key is to couple an analysis of applicable laws and regulations with an analysis of the business.

A single incident can lead to a legal risk that fits into multiple boxes. As an example, contravention of a water quality permit will be a violation and fit into box A. Depending on the mindset of the parties responsible, what would otherwise be a civil liability might evolve into a criminal liability. Further, the same incident can lead to an action by a private party, for example, for trespass (box C).

Practices and procedures currently employed within the Group can be a source of considerable information and can help in undertaking the risk profiling. These include the Insurance Risk Reviews and Disaster Management & Response Programme requirements administered by Group Risk Management, the Human Resource reviews, the Internal Control Questionnaire and the reports prepared by the Group's external auditors. Accordingly, the risk profiling recommended by the guidance may only entail a straightforward gap analysis.

The risk profiling should also result in an assessment of whether or not sufficient policies are in place to address the identified areas of risk.

Irrespective of the methodology employed, any risk profiling or more informal assessment should include a review of the company's past history of incidents and near incidents.

Once a risk profiling exercise is undertaken resort can be had to more traditional and informal mechanisms to ensure the board and management are made aware of changes in the profile. As an example, a number of law firms and other consultants disseminate newsletters and more detailed publications on an ongoing basis. Professional associations in various fields such as accountancy, law and HSE as well as industry groups and trade associations regularly conduct seminars on developing issues. The programme should ensure these resources are accessed.

## Guidelines continued

### **GUIDELINE 3: Incident prevention – training**

Training includes face to face instruction, utilisation of e-learning systems such as CD-ROMs, intranet based training, newsletters and manuals. The use of all such means is encouraged.

A relatively recent development is the advent of Web-based training. LRN of Los Angeles and Rio Tinto have created the Rio Tinto Compliance Training Centre and all Group companies are expected to provide compliance training through the Centre as and when relevant content becomes available.

Training and timeframes within which training must be completed on certain subjects will be mandatory. Timing requirements will be defined in revisions to these guidelines.

The Centre's training content takes the form of individual modules that exist on LRN's dedicated servers. Each module covers a different subject matter. Some of the content is based on discrete areas of law. Other content is more focused on business practices. The system can be accessed via the web allowing employees to dial up from home or to connect through Group networks. Although the system is operated offsite, the employees' perception will be as if they are connecting to their local intranet.

Each module consists of a tutorial and a quiz of ten questions, taking about 35 to 45 minutes to complete. Modules are also available offline.

Training through the Centre is not a total solution but is intended to provide employees with a baseline understanding of those laws and regulations that relate to their job responsibilities. Training can be tailored to the departmental level.

The license with LRN affords the Group the right to 29 LRN library modules, most of which are US based. The license also affords the Group the right to have LRN develop eight personalised modules. A module on *The way we work* and an Australian Trade Practices module have been developed. Additional non US content modules will be developed in the near future.

Further details on course development and server access can be obtained from the head of Compliance.

#### **GUIDELINE 4: Incident prevention – operating procedures**

An example of the type of operating procedures that could be introduced relates to the contracting process.

Presume that through risk profiling a Group company identifies material risks falling into boxes B and/or E of the matrix set out in guideline 2 (contract related risk). That company could then develop procedures to address the key points described below to mitigate the likelihood of occurrence.

The contracting process involves certain key components:

- formulation/negotiation of terms;
- execution;
- administration/monitoring; and
- enforcement and/or defence.

To the extent that systems do not exist, there should be defined approval, review, communication and reporting systems and procedures associated with the entirety of the contracting process, specifying:

- requirements that all agreements be formalised in contract form;
- appropriate delegations of authority;
- adequate communications between production and sales; and
- education on contract terms.

Procedures could be put in place with respect to other types of risks. As an example, many environmental violations (box A in guideline 2), flow from the contravention of permit terms. The

permitting process has similar natural stages and could be made the subject of similar systems and procedures. Similarly, those involved in sales activities may require specific procedures relating to anti-trust or anti-competitive behaviour issues.

## Guidelines continued

### **GUIDELINE 5: Investigations**

The principal purpose of the programme is to prevent incidents of non-compliance, however, this cannot be absolutely guaranteed. Accordingly, rectification/mitigation of the cause and result of an incident and the avoidance of reoccurring violations are also principal goals of the programme. To achieve this material incidents should be subject to root cause investigations.

Failure to properly identify, analyse and classify causes can lead to repeat incidents of non-compliance. Regulators and stakeholders will often excuse violations where it can be established that the incident was either the result of inadvertence or the outcome of a deliberate, unauthorised act. Conversely, regulators will generally be less inclined to provide leeway either in terms of assessing liability or in choosing an appropriate remedy if it is a repeat offence.

In undertaking an investigation the following should be considered:

A number of the standards that define best practice require that all incidents of non-compliance be investigated. In practice this may be unrealistic. However, to ensure the effectiveness of the programme, investigations should be conducted unless:

- the incident was truly immaterial; or
- the committee is satisfied that it knows what happened and why.

An example of the former might be the violation of an effluent limitation set out in a

water quality permit where the incident would not be required to be reported to regulators.

If the committee decides that an investigation is warranted it should be initiated as soon as practicable following the incident.

The investigation should be focused on what happened and, more importantly, the root cause of why it happened.

In seeking to determine root cause, the investigation should focus on and differentiate between behavioural and systemic causes. Often an incident with behavioural roots will be a one off, inadvertent act.

This guideline does not set out express procedures for the conduct of an investigation. Simply put it must be thorough. Interviews and document reviews could play a significant part, but the specific mechanisms and processes to be employed should be left to the committee.

The investigation must help identify necessary and appropriate follow up preventative actions, including modifications to the programme. This is especially relevant to systemic offences.

Any relevant information derived from the *Speak-OUT* programme can be instrumental in the initial stage of investigations.

Employees should not perceive the investigation as a witch hunt. Although such a warning may be viewed as being overly simplistic, if the programme and its purposes are properly publicised at the time of implementation, the investigations should

be seen by employees as an exercise to determine not only what happened, but to make the programme better.

The committee should set the scope of the investigation, commensurate with the violation. This is crucial to ensure that the investigation is effective, and seen as such.

Decisions will need to be taken as to the appropriate individual(s) or entity to conduct the investigation. The range of potential scenarios is too great for this guideline to attempt to detail the makeup of an investigative team. One issue that may arise is the use of legal counsel and legal privilege.

The attorney client privilege is recognised in many of the countries where the Group conducts its business. Although there are differences, the basic purpose of the privilege is to preserve the confidentiality of communications between an attorney (or solicitor or barrister) and his or her client. In circumstances involving corporations, the corporate entity is the client. The privilege extends to any work performed by the attorney, the client or others working under the direction of the attorney, but only to the extent that it is performed to assist the attorney in providing legal advice to the client. Thus, an investigation undertaken under the direction of an attorney for the purposes of providing advice should be privileged. Similarly, the report issuing from the investigation should be privileged.

The following should be borne in mind when attempting to structure an investigation in a manner to take advantage

of the privilege:

- Generally speaking facts are never privileged.
- Although others may be copied with correspondence, this should be limited to only those working for the corporate client who have a decision making role in the underlying matter, or those who are closely involved and whose input is required to progress the investigation.
- Attempts to use the privilege to shield facts or otherwise cloak the investigation in confidentiality where it is not clear that the privilege would be available is seldom a prudent course of action. Improper assertion of privilege can result in its disallowance where it would otherwise be available.
- There may well be times when it would be appropriate to carve out a portion of the investigation and conduct it in such a way that advantage of applicable privileges can be taken.
- In some jurisdictions the law distinguishes between in house and outside counsel, it often being more difficult for the former to avail themselves of legal privileges.

The investigation should result in the issuance of a report to the committee. In addition to the findings and conclusions of the investigating party, the report should set out any recommendations for follow up actions directed at rectifying or mitigating the cause or results of the incident, as well as recommendations directed at avoiding recurrence.

## Guidelines continued

### **GUIDELINE 6: Follow up**

At the completion of an investigation the committee should determine whether to undertake follow up actions directed at rectifying or mitigating the cause (if controllable) and the results of the incident and limiting the prospects of recurrence. The committee should direct the undertaking of any such actions and take the following into consideration.

A decision not to undertake follow up actions should only be made if it is objectively clear that the incident was behaviourally rooted and was so anomalous that follow up would be meaningless. The decision should be supported by the investigative report.

Follow up actions should be tied to the recommendations made in the investigative report and the scope of the actions should be discussed and agreed in writing by the committee. The scope should be in the nature of an action plan. This is especially important where the cause and/or result of the incident is ongoing.

If the incident was rooted, in whole or in part, in systemic failures, attention must be directed at changes in the programme designed to prevent recurrence. These could include modifications to the programme, eg redirected training, as well as changes to operating and business practices.

The decision to modify the programme should be internally well publicised to let employees know that it is directed at making the programme more effective.

If follow up actions will be ongoing, eg if rectification of causes and/or results will require time, targets should be set and monitoring and reporting of progress against those targets should be established.

A report describing the actions undertaken should be prepared following completion of the exercise. The report should clearly detail those actions that are ongoing.

Any modifications to the programme should be accompanied by criteria to allow for the future assessment of their effectiveness. These should be detailed in the report.

### **GUIDELINE 7: Certifications**

The head of Compliance will continue to work with Internal Audit to ensure that the annual Internal Control Questionnaire (ICQ) is the mechanism through which Group company boards and management can certify to the product group chief executive and to the Rio Tinto board that they have implemented and are maintaining the programme.

The ICQ is a de minimus compliance checklist but is not a system in itself. It does not prompt management to probe for gaps in the current risk profile and the policies needed to address them. Nor does it provide for prevention and investigation of non-compliance. The guidance shows the various components needed for a fully functioning system, of which the ICQ is one part.

### **GUIDELINE 8: Adherence assessments**

In undertaking adherence assessments the following should be considered.

#### **Timing and scope**

Adherence assessments should be conducted, at a minimum, on an annual basis.

The scope of the formal adherence assessments should be discussed and agreed by the committee and recorded.

The adherence assessment should look at all aspects of the programme. The exercise should be set against clearly defined criteria and performance measures. Training affords a good example. The committee will have prescribed certain requirements, eg which of the workforce should be trained on what subjects, how long the employee has to complete the training, how often and when retraining is required. If these requirements are not being met, the exercise should attempt to determine the root cause of non-adherence. Similar analyses should be directed at, for example, whether investigations are being initiated within an appropriate time following an incident of non-compliance, whether they are/have been conducted in accordance with the prescribed scope, and whether reports are being issued and acted upon.

Those conducting the adherence assessment should draw on their findings and conclusions and identify possible

## Guidelines continued

remedial and preventive measures, including modifications to the programme.

The adherence assessment should differentiate between individual and systemic issues and, in analysing possible modifications, pay particular focus to the latter.

The exercise should include an analysis of the effectiveness of modifications made as a result of earlier follow up exercises as well as earlier assessments to ensure that the programme is dynamic. Any new recommendations should be accompanied by proposals that would allow for the future assessment of their effectiveness.

The party undertaking the adherence assessment should prepare a report of its findings, conclusions and recommendations. The report should be issued to the committee, and step wise to the board, the product group chief executive, the head of Compliance and the Rio Tinto board or its designees.

### Accountability

Adherence assessments should be the responsibility of the committee. The actual work can be delegated to other personnel within the business, the Rio Tinto Group or to outside consultants. There are a number of factors that militate toward having the exercise performed internally. Chief among these are the following:

- Managers and staff should necessarily have a better understanding of the business and the background and rationale of the programme's requirements;

- Managers and staff should be better able to really assess whether employees are adhering to the programme; and
- Insofar as compliance should be an express job requirement, and, at some level, a managerial accountability, the committee, together with management and staff should be encouraged to assume this responsibility.

Although internally conducted adherence assessments are preferable, there may be associated resource issues. If a Group company is not able to undertake the assessment in a comprehensive manner, it would be preferable to have it undertaken by other qualified Group personnel and/or outside consultants. In this regard it would be acceptable to have the exercise undertaken by internal auditors.

## **GUIDELINE 9: Reviews**

In undertaking reviews the following should be considered.

### **Timing and scope**

Reviews should, at a minimum, be undertaken every two to three years.

The review should be undertaken pursuant to a scope of work discussed and agreed amongst committee members. This should be recorded.

In the context of both effectiveness and relevancy, the review should be set against defined criteria and performance measures, including the programme objectives. It should look at incidents of non-compliance, determine whether they were of the type the programme was intended to prevent and, if so identify and design mechanisms to better ensure prevention. Using training as an example, the review should look at whether the training programmes have had the effect of reducing the incidents of non-compliance in the areas initially targeted by the risk profiling, either in absolute terms or in comparison with our competitors, and, if not, attempt to determine the root cause. Attention should also be paid to incidents or near incidents in areas that have not previously been identified as potentially risky.

The reviewing team should differentiate between individual and systemic issues and, in analysing possible modifications, pay particular attention to the latter.

The review should look at the effectiveness of the programme beyond its

success in preventing non-compliance. As an example, with respect to education of our employees on our key policies, training programmes should have a purely educational purpose. The review should assess whether there is a greater awareness of such policies, irrespective of any related incidents of non-compliance. The review should be targeted at assessing whether the message of and commitment to compliance is being effectively communicated, and if not, what is preventing that from happening.

In the context of relevance, recognition must be given to the fact that neither the legal/regulatory environment, nor our business, is static. Accordingly, the review should look at changes in the law as well as changes in the business and business practices.

In the context of both effectiveness and relevancy, the team conducting the review should identify possible remedial and preventive measures, including modifications to the programme, drawing from their findings and conclusions.

The review should also look at the effectiveness of prior modifications flowing from earlier exercises, including prior reviews, and include recommendations as to how the effectiveness of new modifications can, in turn, be ultimately measured and assessed. Benchmarking against what others are doing in implementing and maintaining a compliance programme is a means of assessing both effectiveness and relevance.

## Guidelines continued

The review should include a strategic analysis of prospective compliance issues. Although this is by definition difficult, it is equally true that trend lines can be identified. This is especially true in the area of compliance as changes to the legal and regulatory landscape are often preceded by public debate.

The party performing the review should prepare a report of its findings and recommendations. The report should be issued to the committee and step wise to the board, the product group chief executive, the head of Compliance and the Rio Tinto board or its designees.

### Accountability

The responsibility to ensure reviews are undertaken lies with the committee. The undertaking of the exercise can be delegated internally or externally. In the context of reviews, however, there is no clear preference for an internally directed exercise. Indeed, it is preferable that other Group personnel or outside consultants be used.

As part of their normal work, the Group's external auditors should assess on a periodic basis whether the programme, as part of a risk management control system, is functioning adequately. Although this assurance is of a higher level than that which the guidance recommends, in the interest of efficiency and given anticipated resource issues Group company boards and the committees may well elect to merge the exercises.

### GUIDELINE 10: Reporting and record keeping

With respect to the reporting and record keeping components of the programme the following should be considered.

#### Reporting

A report should be prepared with respect to the occurrence and/or completion of most of the actions undertaken under the programme. There are multiple reasons for this, namely:

- One of the most important functions of a compliance programme is to prevent systemic problems. Apart from acting as a blueprint for modifications (see below) a report serves as an institutional memory of the action in question, be it the report issuing from the investigation, the report on the follow up actions or other reports prescribed in the guidance. Such institutionalisation should assist in avoiding recurrence;
- The requirement to prepare and issue a report concerning actions undertaken pursuant to the programme should ensure that the appropriate level of discipline and thoroughness is brought to the exercise in question;
- The reports themselves will often serve as the blueprint for next steps; and
- The issuance of reports will substantiate to regulators and other stakeholders that the programme is effective and that the company is exercising due diligence in the management of all aspects of the programme.

As prescribed in the guidance, reports should be prepared in the following contexts, namely:

- *Risk profiling.* A report should be prepared following the completion of the risk profiling exercise. The report should describe the methodology employed; when and by whom it was performed; the findings reached and how such findings will inform programme design, principally training. The report should issue to the committee. Similar reports should issue at any point when the committee undertakes a reassessment of risk.
- *Training.* Periodic reports should be issued to the committee on the various aspects of training programmes, eg how many employees are being trained; from what departments; in what areas; whether training is being completed within the requisite time frames; success rates etc. The Rio Tinto Compliance Training Centre can readily generate reports regarding all such parameters.
- *Incidents.* Reports should be issued to the committee respecting all incidents of non-compliance. They should provide a detailed explanation of the related facts. It is crucial that those issuing the initial report guard against drawing conclusions as to such matters as fault and causation. This is the purpose of the investigation; lack of discipline in this regard could severely prejudice future legal proceedings. Training in the proper conduct of the initial investigation and issuance of the initial

incident report is strongly recommended.

- *Investigations.* A report should be prepared following the completion of the investigations discussed in guideline 5. The report should track and refer back to the initial scope of work. These reports will require much thought in terms of the scope of work. The reasons for this are twofold. First, there may be issues as to the appropriateness of having all or part of the investigation performed by legal counsel so as to allow for the report to be privileged, presuming legal privileges are available. Secondly, in setting the scope of the investigation, the committee should give thought to the type of recommendations they desire from the investigating party. It is not uncommon to see the party conducting the investigation make recommendations as to follow up actions that, for one reason or another, are unrealistic. This often occurs when the investigating party is an outside consultant. It can be prejudicial to receive recommendations that are not subsequently implemented. As with the initial incident report care should be taken in differentiating facts from conclusions and speculation.
- *Follow up.* Presuming follow up actions are undertaken, a report should be prepared that tracks and refers back to the initial scope of work. The report should detail such recommended programme modifications as may be appropriate. As with the follow up exercise itself, particular emphasis should be given to programmatic changes directed at systemic problems.

## Guidelines continued

It should also detail any recommendations pertaining to the means of assessing the effectiveness of such modifications. To the extent that the follow up actions are ongoing, reports should continue on a periodic basis and should include progress against targets.

- *Adherence assessments and reviews.* Reports should be prepared detailing the work performed and the findings, conclusions and recommendations generated from both adherence assessments and reviews. They should track and refer back to the scope of work for the underlying exercises. The reports should include findings and conclusions concerning the effectiveness of those modifications, if any, recommended and implemented as a result of prior adherence assessments and reviews. As with the underlying exercises, particular emphasis should be given in the report to any recommended programmatic changes directed at systemic problems. It should also detail any recommendations pertaining to the means of assessing the effectiveness of such modifications.

### Record keeping

The reports referenced above are records of both the fact that the action in question was undertaken and that the corresponding report was issued. Accordingly, many of the records described in this section would and should take the form of log entries or brief references in committee agendas.

There should be an agenda issued for every committee meeting. The decisions,

deliberations and actions undertaken by the committee as it relates to the design, development, implementation and maintenance of the programme, should be minuted.

## **GUIDELINE 11: Continuous improvement**

Continuous improvement should be achieved through proper management of the programme and by other more traditional mechanisms. The following should be considered.

A number of the programme processes will invariably foster continuous improvement. By definition follow up actions focused on preventing recurrences are directed at improving the programme. Similarly, both the adherence assessments and the reviews are intended to not only identify possible preventive modifications to the programme, but also to assess the effectiveness of previously implemented modifications.

Innovation should be encouraged. This could be achieved through suggestion boxes and the like.

Employees are encouraged to use the *Speak-OUT* Programme to report known or suspected instances of non-compliance. More positively, employees should also be empowered and encouraged to suggest improvements to the programme. Good faith suggestions to improve the programme, whether adopted or not, should be recognised. Consideration could be given to utilising human resource systems to reward innovation.

# 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

Designed by Tor Pettersen & Partners.  
Printed in England by The Beacon Press using their *pureprint* technology.  
© Rio Tinto plc and Rio Tinto Limited.  
10/2003/ENG