

Audit, Risk Management and Sustainability Committee

1. INTRODUCTION AND PURPOSE

This Charter summarises the roles and responsibilities of the Audit, Risk Management and Sustainability Committee of Fortescue Metals Group Ltd (Fortescue or the Company). The disclosure of the role and responsibility of the Committee is designed to inform key stakeholders of the respective accountabilities and contributions of the Committee.

2. ROLE OF THE COMMITTEE

The Audit, Risk Management and Sustainability Committee (Committee) is a committee of Fortescue's Board of Directors (Board). The Committee assists the Board in ensuring:

- effective oversight of the Company's financial, governance and sustainability frameworks; and
- the existence of sound systems of internal control and effective management of risk and compliance.

This Charter provides guidance on the responsibilities of the Committee as determined by the Board. These responsibilities have been allocated to the Committee on the basis that primary responsibility for management of these matters sits with the Chief Executive Officer and the management team.

The Committee shall have full authority and resources to investigate all matters falling within its Charter. The Committee may, at the Company's expense, obtain any external independent professional advice as it considers necessary.

This Charter should be read in conjunction with the Statement of Matters Reserved for the Board and other Board committee charters.

3. MEMBERSHIP AND ATTENDEES

3.1 Membership

The Committee shall consist of at least three non-executive directors appointed by the Board, a majority of whom should be independent directors. Committee members shall possess sound financial management skills and business acumen. Committee members shall hold appropriate formal qualifications.

The Chair of the Board shall not be a member of the Committee but may attend Committee meetings.

3.2 Chairperson

The Chair of the Committee shall be an independent director appointed by the Board. In the temporary absence of the Chair, one of the other Committee members, either nominated by the Chair or elected by the Committee, will act as Chair.

The Committee Chair will attend the annual general meeting of the Company to ensure that any shareholder questions on the Committee's activities can be addressed.

3.3 Quorum

A quorum of the Committee shall be at least two members.

3.4 Other Attendees

Any director who is not a Committee member may attend meetings at their discretion but only as an observer. The Company Secretary of Fortescue shall be the Secretary of the Committee.

For individuals not listed above, attendance at meetings is strictly by invitation only.

4. MEETING FREQUENCY

The Committee shall meet at least four times per annum and at other times as the Chair, a member, or the Secretary of the Committee, requires.

5. REVIEW OF COMMITTEE

5.1 Committee Performance

The Committee Chair shall assess the performance of the Committee on an annual basis and take appropriate action to address desired improvements in respect of areas where there is a need to enhance its role, effectiveness, process or composition.

5.2 Committee Charter

The Committee Chair is responsible for ensuring that the Committee Charter is reviewed at least every other year for the purpose of assessing its continued relevance to the needs of the Board and identifying any enhancements required. Proposed enhancements shall be submitted to the Board for approval.

6. SCOPE

6.1 Corporate Governance

The ASX Corporate Governance Principles and Recommendations (4th Edition) provide fundamental principles for a strong corporate governance framework. While compliance with the ASX Principles is not mandatory, companies are required to report and explain any deviations from the Principles. The Board believes that the Principles represent a sound basis for good governance. As such, the Committee shall have oversight of the Company's compliance with the ASX Corporate Governance Principles and Recommendations (4th Edition).

6.2 Financial Reporting

6.2.1 General

In reviewing and monitoring the Company's financial reports, the Committee shall consider with management the following:

- appropriateness of critical accounting policies, judgments and estimates applied in the preparation of the financial reports;
- alternative accounting policies applied by other companies;
- implications of expected changes in accounting policies;
- significant financial reporting judgments used in preparing the financial reports;
- quality of earnings and the implications of earnings volatility resulting from exceptional and/or non-recurring income and expenditure;
- impact of the Company's financing structure on current and future profitability;
- the effectiveness of financial systems and controls within the Company;
- the ability of the Company to pay its debts as and when they become due and payable;
- the sensitivity of the Company's financial performance to material business risk; and
- the way in which corporate governance matters are disclosed in the financial report.

The Committee shall recommend to the Board that the financial information in the annual and interim reports be approved.

6.2.2 Tax Compliance

In reviewing and monitoring the Company's tax risk management and governance, the Committee shall consider the following:

- assurance as to the operational effectiveness of the Company's tax risk management and compliance framework;
- appropriateness of critical tax policies and judgements applied in the preparation of financial reports and compliance obligations;
- implications of expected changes in prevailing and applicable tax laws to the Company's operating business and structure;
- comfort that the thresholds and timing for escalation of tax risks to the Committee and Board are set at an appropriate level; and
- the Company's tax profile, including its effective tax rate and the basis for any significant deviation from the prevailing corporate tax rate.

6.3 Audit

6.3.1 External Audit

Committee oversight of the external audit function will include:

- recommend to the Board the appointment, reappointment and removal of the external auditor and review their qualifications, objectivity, independence, strategic focus and resources with respect to any services provided to the Company;
- review with the external auditor the scope of their audit and subsequently their audit findings, including any recommendations for improvements in internal controls;
- monitor the effectiveness of the external auditor and the responsiveness of management to their findings and recommendations;
- periodically meet with the external auditor, independently of management, to discuss the quality of the Company's accounting principles, material judgments and any other matters that the Committee or external auditor deem appropriate;
- agree the terms of engagement and approve the fees and other remuneration paid to the external auditor for audit services;
- review and approve the policy for in-advance approval of all audit and non-audit services provided by the external auditor; and
- recommend to the Board the policy for rotation of external audit engagement partners.

6.3.2 Internal Audit

The Company's internal audit function reports directly to the Committee on the outcomes of its reviews. The Board has endorsed an Internal Audit Charter that sets out the requirements of the internal audit function. Day to day management of the internal audit function is the responsibility of the Chief Financial Officer. Committee oversight of the internal audit function shall include:

- approval of the appointment of the Group Manager Risk & Assurance;
- approval of the appointment of any internal audit service providers;
- approval of annual internal audit plans;
- review of reports on the outcomes of internal audit reviews;
- approval of all non-internal audit services provided by any internal audit service provider; and

The Committee will meet independently with the Group Manager Risk & Assurance (including the internal audit service provider where appropriate) at least annually to discuss any significant difficulties encountered, including restrictions on the scope of work, access to required information and any other relevant matters.

6.4 Risk Management and Internal Controls

6.4.1 Risk Management

Committee oversight of Risk Management shall include:

- understand and endorse the Company's risk appetite. Risk appetite is the amount of risk an organisation is willing to accept in pursuit of stakeholder value. The Company's management shall engage with the Committee to establish a mutual understanding of the Company's overall appetite for risks as determined by the Board
- review the extent to which management has established an effective system of risk management and internal control. The Committee shall consider the effectiveness of existing risk management processes and require management to demonstrate the effectiveness of those processes in identifying, assessing and managing the Company's most significant risk exposures.
- review the Company's risk profile by comparison to its risk appetite. Effective oversight of risks is contingent on the ability of the Committee to understand and assess the Company's strategies for managing its critical risk exposures. The Committee shall consider any circumstances where the Company may need to operate outside the agreed risk appetite and whether such circumstances require reporting to the Board.
- undertake periodic review of the Company's most significant risks and whether risk management strategies are appropriate. Risks constantly evolve and regular updating by management to the Committee of key risks and associated risk strategies is critical to effective Board oversight of key risk exposures.

6.4.2 Internal Control Framework

The Committee will monitor the performance of the Company's internal control framework through:

- review of the effectiveness of those internal controls frameworks, processes and systems implemented by management to manage the Company's risk profile;
- understanding the controls and processes implemented by management to ensure that the financial statements derive from the underlying financial systems, comply with relevant standards and requirements, and are subject to appropriate management review; and
- consider whether management has implemented recommendations made by the internal and external auditor and assess the impact of any adverse external and internal audit findings on internal control systems.

6.4.3 Insurance

The Board has delegated specific responsibility to the Committee for oversight of the adequacy of the Group's insurance program and its effectiveness in managing insurable financial risk, where appropriate. Specifically, the Committee will:

- review and endorse the overall strategy for material insurance programs including (but not limited to) Workers Compensation, Industrial Special Risks (property), Public and Products Liability, Directors and Officers Liability, Construction Works & Liability, Marine and Aviation Hull and Liability and Marine Transit;
- review the use of Fortescue's captive insurance company in supporting the overall insurance strategy;
- endorse the renewal and/or placement of all material insurance programs, including associated policy limits, deductibles and premiums;
- approve the appointment and/or removal of Fortescue's insurance broker(s); and
- periodically review the status of risk reduction recommendations made by Fortescue's property insurer.

6.4.4 Cyber Security

The Committee assists the Board, providing oversight of Fortescue's Cyber Security Control framework and the ongoing management of cyber security as a strategic business risk, including data privacy, by ensuring:

- the operational effectiveness of Fortescue's cyber security control framework and the ongoing performance of cyber security strategies and standards;
- the approval of the annual cyber security assurance program, acceptance of related audit findings and the endorsement of any proposed recommendations;
- the consideration of material cyber security risks and understanding of new and emerging cyber security threats and regulatory obligations (national and international);
- an appropriate cyber resilience culture exists built on shared responsibility; and
- review of all material cyber security incidents, plans for remediation and timely disclosure.

6.5 Business Integrity

6.5.1 Anti-Bribery and Corruption

Committee oversight of Anti-Bribery and Corruption (ABAC) compliance shall include:

- review at least annually compliance with the ABAC Policy and ABAC Standard;
- review and report to the Board all breaches of the ABAC Policy notified by management; and

- meet independently with the Company Secretary at least annually to discuss the ABAC compliance framework (incident reporting, risk assessment and training) and any other relevant matters.

6.5.2 Sanctions

Committee oversight of the Sanctions Compliance program shall include:

- review at least annually the compliance with the Sanctions Compliance Policy and Standard;
- review and report to the Board all breaches of the Sanctions Compliance Policy notified by management; and
- meet independently with the Company Secretary at least annually to discuss the Sanctions Compliance framework (incident reporting, risk assessment and training) and any other relevant matters.

6.5.3 Whistleblower Reporting and Investigation

Committee oversight of the whistle-blower compliance framework shall include reviewing all matters reported internally and via the external Whistleblower Hotline.

6.6 Sustainability

6.6.1 Environmental Management

The Board has delegated specific responsibility to the Committee for monitoring the performance of environmental management and related risks and controls through:

- review of regular environmental compliance updates;
- periodic consideration of material risks related to environmental performance and compliance obligations;
- the effectiveness of internal environmental compliance controls implemented by management; and
- assessing the impact of any adverse external regulatory/audit findings on environmental management systems.

6.6.2 Climate Change

The Committee shall provide oversight of Fortescue's response to climate change and provide advice and guidance to the Board on matters associated with:

- developments in the industry regarding regulatory and market responses (both nationally and internationally) associated with climate change and emissions;

- Fortescue's climate change and decarbonisation strategy;
- climate change risk analysis and associated risk mitigation strategies;
- emissions targets and related metrics;
- all climate change and emissions reporting and related disclosures; and
- results of any audits or reviews related to climate change and emissions reporting.

6.6.3 Human Rights and Modern Slavery

The Committee shall provide oversight of Fortescue's human rights risks, including modern slavery, and will provide advice and guidance to the Board on matters associated with:

- Fortescue's compliance with Australia's Modern Slavery Act and equivalent legislation in foreign jurisdictions;
- Fortescue's Human Rights Policy and human rights and modern slavery strategy;
- human rights and modern slavery assessments in Fortescue's global supply chain;
- human rights and modern slavery risk analysis and associated risk mitigation and remediation strategies;
- breaches of Fortescue's Human Rights Policy and plans for remediation;
- effectiveness of human rights and modern slavery due diligence processes and training (internal and with suppliers);
- all human rights and modern slavery reporting and related disclosures; and
- results of any audits or reviews related to human rights and modern slavery.

6.6.4 Indigenous Heritage

The Committee shall provide oversight of Fortescue's commitment to the protection and management of indigenous cultural heritage, and will provide advice and guidance to the Board on matters associated with:

- compliance with and review of domestic and international legislative requirements, or adoption of best practice for cultural heritage management where legislation is absent or not fit for purpose;
- managing heritage risk;
- any breach of legislative requirements and the strategy required for the remediation of the breach;
- compliance with Fortescue's Guidelines for Heritage Management and Protection and the periodic review of the Guidelines to determine their effectiveness; and

- the expectations of the Indigenous People in the protection and management of their cultural heritage and inclusion in advancing and promoting their cultural heritage.

6.6.5 Indigenous Engagement

The Committee shall provide oversight of Fortescue's Indigenous Engagement strategy, and will provide advice and guidance to the Board on matters associated with:

- compliance with Fortescue's native title agreements, including risks associated with breaches and native title party non-compliance;
- indigenous contracting opportunities and performance against targets;
- Fortescue's incorporation of the principle of Free, Prior and Informed Consent into project development and operations;
- conformance with relevant international standards relating to the resources industry working with indigenous communities.

6.6.6 Community Investment

The Committee shall provide oversight of Fortescue's community investment framework, and will provide advice and guidance to the Board ensuring that:

- investment in communities remains strategic and delivers maximum value for the business, community stakeholders and shareholders; and
- investment aligns with our corporate vision and values, ensuring the Fortescue brand and reputation is consistently presented and enhanced.

6.7 Other

The Board may delegate the consideration or review of any specific matter to the Committee as deemed appropriate from time to time.

7. REPORTING TO THE BOARD

7.1 Annual Reporting to the Board

7.1.1 Risk Management and Internal Control

Within the context of the above reporting requirements, the Committee, in accordance with the requirements of the ASX Corporate Governance Principles and Recommendations (4th Edition) related to risk management will, on an annual basis, advise the Board:

- that the Committee has reviewed the Company's risk management framework to satisfy itself that it continues to be sound and that the entity is operating with due regard to the risk appetite set by the Board (Recommendation 7.2); and

- whether it has received assurance from the Chief Executive Officer and the Chief Financial Officer that the declaration provided in accordance with section 295A of the Corporations Act is founded on a sound system of risk management and internal control and that the system is operating effectively (Recommendation 4.2).

These matters must be reported to the Board prior to the Board adopting the audited annual financial report.

7.1.2 Corporate Governance Statement

The Committee will ensure that the following material is included in the Corporate Governance Statement in the Annual Report and/or as separately reported by the Company:

- an explanation of any departures from the ASX Corporate Governance Principles and Recommendations (4th Edition); and
- whether the Company has any material exposure to environmental or social risks and, if it does, how it manages or intends to manage those risks (Recommendation 7.4).

7.2 Periodic Reporting on Committee Activities

The Committee will report to the Board on Committee activities at each Board meeting. Activities to be reported will depend on the Committee's agenda for each meeting. Committee reports will include the following:

- assessment of whether the Company's external financial reporting performance is of the required standard and is adequate for shareholder needs;
- assessment of the strength of the internal control framework based on the outcomes of internal audit reviews;
- assessment of the performance of management in addressing material business risks;
- processes and controls related to the selection and appointment of the external auditor, maintenance of the external auditor's independence and compliance with the engagement partner rotation policy;
- recommendations for the appointment or, if necessary, the removal of the external auditor;
- assessment of the performance and independence of the external auditor; and
- assessment of the performance of the internal audit function and recommendations for the appointment or, if necessary, the removal of the internal audit service providers.

This Charter was approved by the Board in April 2021.