

RISK AND COMPLIANCE COMMITTEE CHARTER

(Approved by the Board on 21 August 2020)

1. INTRODUCTION

The purpose of this Charter is to document the objectives, responsibilities, composition and administration of the Risk and Compliance Committee (**Committee**) of the Board of the Australian Institute of Company Directors (**AICD**).

Defined terms in this Charter have the same meaning as in the AICD Constitution.

2. OBJECTIVES

The objectives of the Committee are to assist the Board to discharge its corporate governance responsibilities to exercise due care, diligence and skill in relation to oversight of the design, quality, effectiveness and integrity of the AICD's risk management strategy, Risk Management Framework and overall risk management; and the Compliance Framework.

3. DUTIES AND RESPONSIBILITIES

3.1 The Committee considers any matters necessary in order to fulfil its objectives and makes recommendations to the Board. The Committee also examines any other matters referred to it by the Board.

3.2 Risks, Policies and Controls

The main duties and responsibilities of the Committee in relation to risks, compliance, policies and controls are to:

- (a) Review AICD's risk management strategy and Risk Management Framework (including the risk appetite statement) at least annually to ensure its continued application and relevance;
- (b) Review the adequacy and currency of the AICD's risk management policies, and other policies as relevant;
- (c) Monitor the adequacy and effectiveness of the AICD's risk management processes;
- (d) Review the effectiveness of the Risk Management Framework for identifying, monitoring and managing compliance with relevant compliance obligations;
- (e) Make recommendations to the Board regarding the AICD's emerging and material risks including to the AICD budget or strategy, or other particular risks or risk management practices including mitigation of such risks;
- (f) Review the adequacy of the IT Governance Framework and monitor the control systems in place, including reviewing the external IT auditor's written reports and monitoring responses and actions to correct any deficiencies;
- (g) Prior to the AICD implementing substantial new IT solutions, review and approve the due diligence and risk assessment of any proposal where sensitive or privacy related data will be recorded (including in a Cloud application) and such assessment is rated high or very high;
- (h) Review the effectiveness of the AICD's risk management processes for managing actual, suspected or alleged fraud or corruption affecting the AICD;
- (i) Review copies of internal and external audit reports where risk issues have been the subject of the audit; and

RISK AND COMPLIANCE COMMITTEE CHARTER

- (j) Review Management's annual attestations.

3.3 Compliance with Legal and Regulatory Obligations

The Committee will:

- (a) Review at least annually, the AICD's Compliance Framework and provide recommendations to the Board.
- (b) Review the effectiveness of the Compliance Framework for identifying, monitoring and managing compliance with relevant obligations.
- (c) Consider the adequacy of processes for reporting and responding to legal and regulatory breaches and complaints, including monitoring the operation of the AICD's Whistleblower Policy.
- (d) Review reports under the Compliance program, including any investigations into compliance incidents.
- (e) Undertake any other work requested by the Board from time to time in connection with compliance activities.
- (f) Review copies of internal and external audit reports where compliance issues have been the subject of the audit.

3.4 Insurance

The Committee will:

- (a) Review and approve the AICD's insurance coverage;
- (b) Review the AICD's insurance program to ensure it meets the AICD's needs and aligns with the AICD's risk appetite and profile;
- (c) Identify any special projects or investigations relating to insurance deemed necessary;

3.5 Reporting

The Committee will have oversight of, and review the regular reporting on:

- (a) Compliance incidents;
- (b) Operational incidents;
- (c) Complaints;
- (d) Work, Health and Safety (WHS) processes;
- (e) Legal and regulatory updates;
- (f) Litigation; and
- (g) Whistleblower matters.

4. COMPOSITION AND MEETINGS

4.1 Membership and Attendance at Meetings

- (a) The Committee comprises at least three (3) members (all of whom are non-executive Directors and a majority of whom are independent Directors) including:
 - (i) The Chair of the Committee (**Committee Chair**) who is to be an independent member of the Board, appointed by the Board, but must not be the Chair of the Board; and

RISK AND COMPLIANCE COMMITTEE CHARTER

- (ii) At least two (2) other members of the Board as appointed by the Board, and any other parties nominated by the Board.
- (b) A quorum of the Committee is any two (2) members of the Committee.
- (c) All Directors can attend Committee meetings. Notice of Committee meetings will also be provided to the Chief Executive Officer (**CEO**), Chief Financial Officer (**CFO**) and General Manager Corporate Services and the Head of Risk & Compliance. Other members of Management and advisors can also be invited to attend meetings as the Committee Chair thinks fit.
- (d) The secretary of the Committee is the Company Secretary, or another person nominated by the Committee Chair.

4.2 Meetings

- (a) Meetings of the Committee are held at least four (4) times per year. The Committee also meets at the request of the Board, any Committee member, any other non-Committee Board member, the CEO or the Company Secretary.
- (b) Meetings can be held in person, by telephone or by video conference, or by any combination of these media.
- (c) The secretary, or other person nominated by the Committee Chair, takes minutes of the proceedings of all meetings of the Committee.

4.3 Authority

- (a) The Board has absolute authority over the Committee's findings and recommendations.
- (b) The Board delegates authority to the Committee, within the scope of its responsibilities, to:
 - (i) Obtain any information it requires from any employee or external party, including interviewing Management and internal and external auditors (with or without Management present);
 - (ii) Obtain outside legal or other independent professional advice; and
 - (iii) Facilitate the attendance at Committee Meetings of external parties with relevant experience and expertise.

4.4 Consultation

The Committee Chair will liaise and consult with the chair of the Audit, Finance & Investment Committee quarterly or more frequently as deemed necessary to fulfil the objectives of the Committee.

4.5 Sub-delegation

The Committee may, at its discretion, delegate some or all of its responsibilities to the Committee Chair or a sub-committee of the Committee.

4.6 Board Reporting

The Committee Chair reports to the Board after each meeting of the Committee. The report must cover the findings and recommendations of the Committee. The minutes of all Committee meetings must be circulated to the Board.

RISK AND COMPLIANCE COMMITTEE CHARTER

4.7 Review of Charter, Committee Composition and Committee Performance

- (a) The Committee will at least annually review its composition and Charter and recommend any changes to the Board.
- (b) The Board will at least annually review the composition of the Committee and the Committee Charter.
- (c) The Committee will at least annually review its performance as a Committee.