

## Risk & Compliance Committee Charter

---

The role of the Risk & Compliance Committee (Committee) is documented in this Board approved Charter.

1. The primary role of the Committee is to oversee and monitor the effectiveness of GMHBA's risk management framework and to assist the Board in the identification, management and mitigation of material risks.

### Scope

2. GMHBA Limited, including all private health insurance businesses, health related businesses and any subsidiary entities.
3. Clinical risk management is a component of the risk management framework and is within the scope of this Committee, supported by the internal Clinical Quality & Risk Committee and the external Clinical Advisory Committee.

### Objectives

4. The objectives of the Committee are to:
  - assess and report to the Board on the status of material business risks to the organisation through an integrated and mature enterprise risk management framework;
  - identify and oversee risks and circumstances that may impede the performance or execution of the strategic plan or affect the overall sustainability of the organisation;
  - monitor the organisational risk profile relative to the Board approved risk appetite; and
  - support and promote a risk-aware culture throughout the organisation.

### Composition

5. The Committee must comprise at least three and not more than four directors, all of whom must be non-executive directors and free from any relationship which might in the opinion of the Board be construed as a conflict of interest. Where possible a director with medical or clinical experience should be a Committee member.
6. The Committee may elect one member as the Committee Chair. The Committee Chair must not also be the Chair of the Board.
7. Committee membership may include non-director independent person(s) in accordance with whatever arrangements for such appointments are approved by the Board from time to time. Any such appointees are eligible to attend Committee meetings but are not counted towards a quorum and only directors may participate in decisions.
8. The Chief Executive Officer, Chief Risk Officer, Head of Compliance, Company Secretary and any other Executive(s) or senior staff responsible for key aspects of enterprise-wide risk management are required to attend all Committee meetings.

### Duties and Responsibilities

9. The duties and responsibilities of the Committee are:

#### **9.1. General risk oversight and monitoring**

- assist the Board in setting risk appetite and tolerance levels within management shall operate;
- assist management and the Board in identifying and managing material strategic and operational risks and oversee that these risks are appropriately mitigated through effective controls;
- monitor the effective implementation of the Risk Management Strategy; and
- oversee risk culture and risk maturity at GMHBA including reviewing the results of the risk culture survey.

## Risk & Compliance Committee Charter

---

### 9.2. Internal control and risk management

- oversee internal processes for determining and managing key risk areas;
- oversee the effectiveness of the internal control, risk management and performance management reporting systems, including the quality, type and presentation of risk-related information provided to the Board;
- liaise with the Audit & Investment Committee as appropriate to obtain comfort that:
  - internal controls identified as important to risk management are within the scope of the Audit & Investment Committee oversight; and
  - reports to the Audit & Investment Committee from internal or external auditors that identify material risks are shared with the Committee for its additional oversight.
- review and endorse to the Board (with support from an external expert if required) GMHBA's Disaster Recovery Plan and Business Continuity Plan, including tolerance levels for disruptions to critical operations, and review the results of testing;
- review and approve the Group Fraud and Corruption Policy, monitor GMHBA's exposure to fraud and review reports on any major frauds or thefts;
- review and approve the OH&S Policy and related Policies; and
- review and approve the Group Whistleblower Policy and oversee the effectiveness of the whistleblower program including assessing any disclosures received internally or through the external FairCall service.
- oversee GMHBA's management of Material Service Providers by approving the Service Provider Policy and reviewing risk and performance reporting on material service providers.

### 9.3. Compliance

- monitor the effectiveness of GMHBA's approach to achieving compliance with laws, regulations, industry codes and Group policies;
- review any significant changes to legislative or regulatory requirements that impact compliance frameworks or controls; and
- review any regulatory correspondence relating to areas of material risk; and
- receive management reporting on relevant compliance topics.

### 9.4. Governance

- develop an annual work plan for the Committee.
- review the Committee Charter every two years or more often in the case of regulatory or other change.
- regularly evaluate the performance of the Committee.

### Meetings

10. The Committee will hold at least three meetings per year, and such additional meetings as the Committee Chair shall decide are necessary for the Committee to fulfil its duties.
11. The Committee Chair is required to call a meeting of the Committee if requested to do so by any Committee Member, the Chief Executive Officer, the Chief Risk Officer or the Board.
12. The Company Secretary will act as Committee Secretary and is responsible, in conjunction with the Committee Chair and relevant executives, for preparing and circulating the agenda and meeting materials to Committee members at least four working days prior to a meeting.
13. The Company Secretary will prepare minutes of each Committee meeting as well as a summary to be submitted to the next Board meeting for information.
14. Two members of the Committee constitutes a quorum.

## Risk & Compliance Committee Charter

---

### Access

15. The Committee shall have direct and unfettered access to all executives as well as to the internal and external auditor and the Appointed Actuary, and executives shall have direct access to the Committee via the Company Secretary.
16. The Committee may consult or retain independent experts where it is considered necessary and in accordance with whatever arrangements are approved by the Board from time to time.

### Other Matters

17. Where able to do so, Committee members will:
  - assist with bringing to the Committee information they may come across as to best practice in respect of risk management practices and procedures, or approaches to compliance; and
  - alert the Committee to any relevant emerging risks or changes to the environment in which the company operates of which they become aware.

Approved December 2024