Risk & Compliance Committee Charter

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

2. The primary role of the Committee is to oversee and monitor the operation of the company's risk management framework and to assist the Board in the exercising of due care, diligence and skill in relation to the identification, management and mitigation of material risks.

Scope

3. The scope of the Committee covers GMHBA Limited, including all private health insurance businesses, health related businesses and wholly controlled entities.

4. Clinical risk management is a component of the enterprise wide 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

5. 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 enterprise risk management framework aimed at ensuring risks are identified, assessed and appropriately managed via operational risk management frameworks based on industry accepted and regulatory standards;
   - monitor and review issues/risks that may impede the goals, objectives and performance of the organisation;
   - monitor the company's risk profile relative to the Board approved risk appetite; and
   - consider and assess that an appropriate risk-aware culture has been embedded throughout the company.

Composition

6. 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.

7. Committee members may elect one of their number as the Committee Chairman. The Committee Chairman must not also be the Chairman of the Board.

8. Committee composition may include non-director independent person(s) in accordance with whatever arrangements for such appointments are approved by the Board from time to time, provided that the number of non-director independent members does not equal or exceed the number of director members.

9. The Chief Executive Officer, Chief Risk Officer, Risk Manager, Compliance Manager, Company Secretary and any other Executive(s) or senior staff responsible for key aspects of enterprise wide risk management are invited to Committee meetings at the discretion of the Committee Chairman.

Duties and Responsibilities

10. The duties and responsibilities of the Committee are:

10.1. General risk oversight and monitoring

- assist the Board in setting risk appetite and tolerance levels within which the GMHBA Limited Group, GMHBA Limited fund and the health.com.au fund shall operate;
- assist management and the Board in identifying and considering strategic and operational risks and ensure that these risks are appropriately reflected in the risk management policies, plans and processes;

- monitor the effective implementation of the risk management strategy; and
- oversee the risk culture and risk maturity of the Group and entities.

From time to time the Committee may act on the Board's behalf in the control and implementation of specific projects subject to whatever delegated authority the Board establishes for that project.

10.2. Internal control and risk management

- assess the internal processes for determining and managing key risk areas;
- address 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 Committee as appropriate to obtain comfort that:
    - internal controls that have been identified as important to the management of risk have been included within the scope of the Audit Committee oversight; and
    - reports to the Audit Committee from internal or external auditors on the control environment are shared with the Committee as far as is relevant to the assessment of the effectiveness of the risk management frameworks.
- review and monitor risk management and internal compliance and control systems as part of monitoring the appropriateness of the internal control framework;
- review and endorse (with support from an external expert) the company's Disaster Recovery Plan and Business Continuity Plan;
- review and approve the Group Fraud and Corruption Policy, and evaluate the company's exposure to fraud and review reports on any major frauds or thefts from the company;
- 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 reviewing any disclosures received via internal disclosure or through the external FairCall service.

10.3. Compliance

- monitor the effectiveness of the Group's approach to achieving compliance with laws, regulations, industry codes and Group policies;
- review any significant changes to legislative or regulatory requirements that may impact compliance frameworks or systems;
- review correspondence from regulatory bodies on significant issues; and
- receive reports from managers regarding compliance within their part of the business.

10.4. 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

11. The Committee will hold at least four regular meetings per year, and such additional meetings as the Committee Chairman shall decide are necessary for the Committee to fulfil its duties.

12. The Committee Chairman 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.

13. The Company Secretary will act as Committee Secretary and is responsible, in conjunction with the Committee Chairman and relevant executives, for preparing and circulating the agenda and meeting materials to Committee members, at least four working days prior to the meeting.

14. The Company Secretary will prepare minutes of each Committee meeting together with any major reports considered at those meetings, as well as a summary to be submitted to the next Board meeting for information.

15. A quorum shall consist of two members of the Committee.

Access

16. The Committee shall have direct and unfettered access to the executives as set out above, as well as to the internal auditor and the Appointed Actuary, and those executives and others shall have direct access to the Committee via the Committee Chairman.

17. The Committee may consult or retain independent experts where they consider it necessary to carry out their duties and in accordance with whatever arrangements are approved by the Board from time to time.

Other Matters

18. 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 2020