# Risk Management Committee Charter

Medibank Private Limited (ABN 47 080 890 259) **("Medibank")**

# Risk Management Committee Charter

## 1 PURPOSE AND AUTHORITY

### 1.1 Purpose

The purpose of this Risk Management Committee Charter is to set out the authority delegated to the Risk Management Committee ("**Committee**") by the Board of Directors of Medibank ("**Board**") and to set out the role, responsibilities, membership and operation of the Committee.

### 1.2 Authority

The Committee is a committee of the Board established in accordance with Medibank's constitution and is authorised by the Board to assist it in fulfilling its risk management responsibilities.

It has the authority and power to exercise the role and responsibilities set out in this Charter and under any separate resolutions of the Board granted to it from time to time.

## 2 ROLE OF THE COMMITTEE

The role of the Committee is to assist the Board by providing objective, non-executive oversight of the implementation and operation of Medibank's risk management framework, and compliance by Medibank with the Australian Prudential Regulation Authority ("**APRA"**) Consolidated Prudential Standard 220 Risk Management ("**CPS220**"), to monitor that risk taking in Medibank is conducted within reasonable bounds and that financial and non-financial risks are clearly identified and well managed.

In fulfilling this role, the Committee will – in accordance with Medibank's purpose, values and Code of Conduct – have appropriate regard to customer and community interests and expectations.

## 3 RESPONSIBILITIES

### 3.1 Risk culture

The Committee is responsible for monitoring and reviewing Medibank's risk culture and making recommendations to the Board on:

(a) the overall policy direction of the Group Risk and Group Compliance functions;

(b) the attitude and appetite for risk within Medibank, and the extent to which the risk culture supports Medibank's ability to operate consistently within its risk appetite; and

(c) any desirable changes to risk culture, to facilitate a strong risk culture being maintained.

### 3.2 Risk management framework

The Committee is responsible for:

(a) overseeing the implementation and operation of the risk management framework, the compliance management framework and other internal compliance and control policies, frameworks and systems to ensure effective management of financial and non-financial risks (including but not limited to clinical, compliance and operational risks);

(b) ensuring that Medibank's risk management framework is:

  (i) reviewed at least annually to satisfy the Committee that it continues to be sound and that Medibank is operating with due regard to the risk appetite set by the Board; and

  (ii) subject to any other external reviews required in accordance with CPS220;

(c) monitoring the effectiveness of Medibank's risk management framework and compliance management framework, including monitoring the outcomes from the annual review by the internal or external auditors of the Medibank's risk management framework as reported to the Audit Committee;

(d) considering reports from management on new and emerging sources of risk and the controls and mitigation measures that management has put in place to deal with those risks;

(e) considering the results of an independent comprehensive review of the appropriateness, effectiveness and adequacy of the risk management framework conducted periodically; and

(f) making recommendations to the Board for approval on Medibank's risk management framework (including the Risk Management Strategy, Risk Appetite Statement Framework, Risk Appetite Statement Policy, Risk Culture Framework and Risk Management Procedure).

### 3.3 Risk profile and appetite

The Committee is responsible for:

(a) advising the Board on Medibank's overall current and future risk appetite and recommending Medibank's risk appetite statement to the Board for approval;

(b) overseeing Medibank's current and future risk position relative to its risk appetite and capital strength; and

(c) monitoring Medibank's risk profile and material risk categories for consistency with the risk appetite statement.

### 3.4 Risk management

The Committee is responsible for:

(a) overseeing senior management's implementation of Medibank's risk management strategy, including senior management's monitoring and managing of Medibank's material risks, consistent with strategic objectives, risk appetite statement and key policies;

(b) overseeing stress testing of Medibank's key risks including both scenario analysis and/or sensitivity analysis, where applicable;

(c) constructively challenging senior management's proposals and decisions on all material aspects of risk management arising from Medibank's activities;

(d) considering reports concerning material risk events (including but not limited to fraud) and overseeing management's process for ensuring that the issues identified (including underlying causes) are addressed in an appropriate and timely manner;

(e) reporting to and consulting with the People and Remuneration Committee to enable risk outcomes to be appropriately reflected in remuneration outcomes and as necessary, to maintain the linkage between risk and remuneration;

(f) referring to the Audit Committee and Investment and Capital Committee any matters that have come to the attention of the Committee that are relevant to those committees;

(g) approving material risk management and compliance policies which support the enterprise risk management framework;

(h) monitoring that Medibank has in place appropriate systems and procedures to ensure compliance with all relevant laws, regulations, codes and standards;

(i) reviewing anti-bribery and anti-corruption, fraud control and whistleblower policies and monitoring Medibank's process for ensuring employees are aware of these policies and dealing with the matters raised by employees under these policies (including breaches of these policies);

(j) monitoring and reviewing whether the operational structure of Medibank facilitates effective risk management and there are sufficient resources dedicated to risk management;

(k) recommending the annual APRA risk management declaration to the Board for approval, as necessary;

(l) reviewing any material insurance matters including, as appropriate, insurance programs and deeds of indemnity, insurance and access;

(m) reviewing the Outsourcing Policy and the material outsourcing arrangements and associated risks and making recommendations to the Board for approval and consideration;

(n) reviewing the Business Continuity Management Policy (and making recommendations to the Board for its approval and consideration) and overseeing the quality of business resilience management (including business continuity, crisis management and disaster recovery); and

(o) reviewing and ensuring appropriate disclosures are made regarding any material exposure Medibank has to economic, environmental and social sustainability risks.

### 3.5 Chief Risk Officer ("CRO")

The Committee is responsible for:

(a) having oversight of, and providing prior endorsement of, the appointment and replacement of the CRO;

(b) reviewing the performance of, and setting the objectives for, the CRO; and

(c) taking reasonable steps to ensure the CRO has unfettered access to the Board and its committees.

## 4 MEMBERSHIP

### 4.1 Composition and size

The Committee is appointed by the Board and will consist of at least three members:

(a) all of whom are non-executive directors;

(b) a majority of whom are independent directors; and

(c) at least one of whom will be a member of the Audit Committee.

Each member must be free from any interest, business or other relationship which, in the opinion of the Board, could, or could reasonably be perceived to, materially interfere with the exercise of his or her independent judgment as a member of the Committee.

The members of the Committee shall have the necessary knowledge and a sufficient understanding of the industry in which Medibank operates to be able to discharge the Committee's mandate effectively.

A member may retire from the Committee by giving written notice to the Chair of the Committee or the secretary of the Committee.

### 4.2 Chair

The Chair of the Committee must be an independent non-executive director, and must not be the Chair of the Board; however, the Chair of the Board may sit on the Committee.

The Chair of the Committee is appointed by the Board.

If, for a particular Committee meeting, the Chair of the Committee is not present within 10 minutes of the nominated starting time of the meeting, or is unable to attend the meeting, the Committee may elect a chair for the meeting.

### 4.3 Secretary

The Company Secretary is the secretary of the Committee.

## 5 COMMITTEE MEETINGS AND PROCESSES

### 5.1 Meetings

Meetings and proceedings of the Committee are governed by the provisions in Medibank's constitution regulating meetings and proceedings of the Board and committees of the Board in so far as they are applicable and not inconsistent with this charter.

Committee members may attend meetings in person or by electronic means.

Committee members must be available to meet with external bodies and regulators if requested to do so in accordance with relevant laws, regulations or prudential standards.

### 5.2 Frequency and calling of meetings

The Committee will meet a minimum of four times each year, and otherwise as frequently as required to undertake its role effectively.

Additional Committee meetings may be convened as the Chair of the Committee considers necessary, taking into account requests from any member of the Committee, the Chief Executive Officer ("**CEO"**), the Group Lead - Chief Financial Officer and Group Strategy ("**CFO"**), the Group Lead – Trust, Legal & Compliance, the Chief Actuary, the CRO, the Hub Lead – Internal Audit, the Hub Lead - Group Compliance or external auditors.

In cases where circumstances make it impractical to convene and hold a meeting, the Committee may pass resolutions by each member signing a circular resolution.

### 5.3 Quorum

Two Committee members constitute a quorum for meetings of the Committee.

### 5.4 Attendance by management and advisors

The Committee must invite the CRO to attend all relevant sections of the meetings. The CEO, CFO, Group Lead – Trust, Legal & Compliance, Chief Actuary, Hub Lead – Internal Audit, Hub Lead - Group, Compliance, clinical governance experts, the Group Chief Medical Officer and external auditors may attend Committee meetings by standing invitation.

The Chair of the Committee may also invite directors who are not members of the Committee, other senior managers and external advisors to attend meetings of the Committee.

### 5.5 Reporting

The Committee through its Chair, will:

(a) report to the Board on its activities on a regular basis; and

(b) take reasonable steps to ensure the Board is aware of material matters considered by the Committee.

### 5.6 Minutes

The secretary of the Committee will keep minutes to record the proceedings and resolutions of Committee meetings, and the minutes will be available to the Board on request.

### 5.7 Access to information and advisors

The Committee has direct and unlimited access to all resources necessary to discharge its duties and responsibilities. This includes:

(a) requiring management or others to attend meetings and to provide any information or advice that the Committee requires;

(b) accessing Medibank's documents and records;

(c) obtaining the advice of special or independent counsel, accountants or other experts, without seeking approval of the Board or management; and

(d) having unfettered access at all times to senior management, the CRO, the Chief Actuary, the Hub Lead – Internal Audit, the Hub Lead - Group Compliance, the Group Chief Medical Officer, external auditors, and heads of all other risk management functions as applicable.

The Committee also has the authority to conduct or direct any investigation required to fulfil its responsibilities.

## 6 COMMITTEE'S PERFORMANCE EVALUATION

The Company Secretary will facilitate a review of the performance of the Committee annually in accordance with processes established by the Board and will report the findings of that review to the Committee and the Board.

## 7 REVIEW AND PUBLICATION OF CHARTER

The Committee will review its charter from time to time to keep it up to date and consistent with the Committee's authority, objectives and responsibilities and report to the Board any changes it considers should be made.

This charter may be amended by resolution of the Board. The Committee may approve non-material or administrative amendments to this charter and report these to the Board.