

SUN LIFE MALAYSIA TAKAFUL BERHAD

Registration No. 200501012215 (689263-M)

CHARTER OF THE RISK MANAGEMENT COMMITTEE**1 Purpose**

The Risk Management Committee (RMC or the Committee) is a standing committee of the Board of Directors (the Board) whose primary objective is to oversee Senior Management's activities in managing the key risk areas of the Company and to ensure that an appropriate risk management process is in place and functioning effectively.

2 Membership

The Board shall establish RMC comprising: -

2.1 Members:

- 2.1.1 at least three (3) directors;
- 2.1.2 a majority of independent directors;
- 2.1.3 be chaired by an independent director; and
- 2.1.4 directors who have the skills, knowledge and experience relevant to the responsibilities of the board committee.

2.2 Permanent Invitees:

- 2.2.1 Chief Executive Officer
- 2.2.2 Chief Executive Officer, Sun Life Malaysia Assurance Berhad (SLMA)
- 2.2.3 Chief Financial Officer, SLMA
- 2.2.4 Chief Risk Officer or equivalent
- 2.2.5 General Counsel, SLMA
- 2.2.6 Chief Compliance Officer or equivalent
- 2.2.7 Appointed Actuary

3 Committee's Duties and Responsibilities

The Committee is responsible for:

3.1 Risk Management

- 3.1.1 reviewing and recommending risk management strategies, policies, risk tolerance and risk appetite that includes considerations on Environmental, Social and Governance (ESG) and climate-related risks for the Board's approval;
- 3.1.2 reviewing at a minimum annually, and assessing the adequacy of Compliance with Risk Management Policies and its frameworks to identify, measure, monitor and control risks as well as the extent of these operating effectively;
- 3.1.3 ensuring adequate infrastructure, resources and or systems are in place to support effective risk management (e.g. ensuring an employee responsible for implementing risk management systems performs those duties independently taking into account the Company's risk taking activities);

- 3.1.4 ensuring that the Chief Risk Officer or equivalent have adequate authority, independence and resources to perform the mandates;
- 3.1.5 reviewing Management's periodic reports on risk exposure, risk portfolio composition and risk management activities;
- 3.1.6 reviewing and assessing on matters set out in clauses 6.4 and 6.5 in the Shareholders Agreement, as recommended by the Executive Committee, for the Board's approval.
- 3.1.7 reviewing the performance of the Enterprise Risk Management Committee (ERMC), the Asset and Liability Committee (ALCO) and the Investment Committee (IC) within the context of the Company's strategy, risk appetite and charter of the respective Committees;
- 3.1.8 reviewing and assessing the results of the stress and scenario testing that includes assessment of climate risks, before endorsing for approval by the Board. In addition, ensuring timely identification and continuous monitoring of suitable corrective action plan by the senior management in addressing the identified risks;
- 3.1.9 reviewing annually key risk-related issues, including the ESG and climate-related risks, incorporated into the business plan;
- 3.1.10 reviewing management's actions related to product design through the processes set out in the Risk Management Policies; and
- 3.1.11 In assisting the implementation of a sound remuneration system and without prejudice to the tasks of the Nomination and Remuneration Committee, examining whether incentives provided by the remuneration system take into consideration risks, capital, liquidity and the likelihood and or timing of earnings.

3.2 Compliance

- 3.2.1 reviewing at a minimum annually, and approving changes to compliance-related policies and or programmes that provide for the monitoring of compliance with legal and regulatory requirements, including legislative compliance within the company's risk management frameworks and internal controls;
- 3.2.2 reviewing at a minimum annually, the adequacy of complying with the Company's Code of Conduct and its enterprise-wide policies for the management, mitigation of compliance risk, which consists of financial crimes risk (including money laundering, terrorist financing, and sanction risk, which encompasses proliferation financing bribery and corruption risk), market conduct risk, privacy risk, and business conduct risk;
- 3.2.3 reviewing quarterly compliance reports presented to the Committee with respect to, among other things, compliance trends and themes on enterprise-wide basis, regulatory reviews and compliance risks and programmes;
- 3.2.4 ensuring adequate infrastructure, resources and systems are in place for an effective compliance risk management (e.g. ensuring that the employee responsible for implementing compliance risk management systems perform duties independently taking into account the Company's compliance risk taking activities); and

- 3.2.5 ensuring that the Chief Compliance Officer or equivalent has adequate authority, independence, and resources to perform the mandates.

3.3 Governance

- 3.3.1 reviewing at a minimum annually, and approving changes to the statements of mandate, responsibility and authority of the Chief Risk Officer or equivalent and Chief Compliance Officer or equivalent; and
- 3.3.2 reviews and recommend to the Board of Directors for approval, the appointment, initial remuneration and termination of the Chief Risk Officer or equivalent and the Chief Compliance Officer or equivalent.

4 Authority

The Committee is authorised by the Board:

- 4.1 to approve the Charter of the ERM, the ALCO and the IC, including delegated responsibility to manage the risk profile of the Company;
- 4.2 to request and receive any management information required to support its risk management oversight activities, as well as to invite any person to be in attendance or seek the advice of professionals in specific areas of expertise it considers necessary in carrying out its duties; and
- 4.3 to provide overall oversight on IT related matters including ex-ante risk assessments on IT applications and to designate Senior Management (C-Suite level) to be responsible for the overall IT risk controls and security.

5 Structure and Operations

5.1 Frequency of Meetings

The Committee shall hold regular meetings, at a minimum once every quarter and shall report regularly to the Board.

In the absence of a meeting, issues shall be resolved by way of circular resolutions and decisions shall be unanimous. The circular resolutions may consist of several documents in the same form, each executed by one or more of the members of the Committee. Any such resolutions may be transmitted by the members of the Committee via email to the Secretary or any other appropriate means.

5.2 Private Session

At each meeting, the Committee holds a separate private session with the Chief Risk Officer or equivalent, and Chief Compliance Officer or equivalent. Each of these has unrestricted access to Committee members between meetings.

5.3 **Quorum**

The quorum necessary for the transaction of business shall be two (2) members. A duly convened meeting of the Committee at which a quorum is present shall be competent to exercise all or any of the authorities, powers and discretions vested in or exercisable by the Committee.

In case the Chairperson of the Committee is on leave or unable to exercise his/her powers for any cause, the Chairperson shall appoint a Director to act on his/her behalf. In the absence of such an appointment, the Directors shall elect from amongst themselves one (1) person to act on behalf of the Chairperson.

All decisions at the meetings of the Committee shall be decided by a simple majority.

5.4 **Secretary**

The Company Secretary or a representative from the Company Secretarial Department shall act as the Secretary of the Committee.

5.5 **Other**

On an annual basis, the Committee shall review the Charter and where necessary, recommend for changes, where deemed fit, to the Board for approval.

The Committee shall undertake and review with the Board on annual performance evaluation of the Committee.

The Chair of the Committee is consulted in advance in connection with the appointment, reassignment, replacement and dismissal of the Chief Risk Officer or equivalent as well as the Chief Compliance Officer or equivalent and annually on the performance assessment and compensation awarded to them.

- END -