Risk Committee Charter

SUNCORP

ISSUE DATE: 6 AUGUST 2021

Introduction

This is the Charter of the Risk Committee. The Risk Committee, appointed by the Board of the Company specified in item 1 of the Schedule also operates as the Risk Committee for the Group, and performs the functions outlined in this Charter, for each of the entities (if any) specified in item 2 of the Schedule except where the entity specified in item 2 of the Schedule has appointed its own risk committee.

The purpose of the Risk Committee is to provide oversight across the Group for all categories of risk, including risk culture. In this role, the Risk Committee has the delegated authority from the Board to approve and oversee the processes used to identify, evaluate and manage risk. At its discretion, the Risk Committee may make recommendations to the Board, including recommendation of the Group's risk appetite.

Definitions

The following terms have the following meanings:

"**Board**" means the board of the Company and the board of each of the entities specified in item 2 of the Schedule, except for those entities which have appointed their own risk committee or adopted their own risk committee charter.

"**Company**" means the company specified in item 1 of the Schedule.

"**Company Secretary**" means the company secretary of the Company.

"**Group**" means the company specified in item 1 of the Schedule and the entities (if any) specified in item 2 of the Schedule.

"**Group Executive**" means senior executive positions directly reporting to the Group CEO & Managing Director.

"**Risk Committee**" means the risk committee of the Group.

"**Suncorp Group**" means the Suncorp Group Limited group of companies.

Role

The Risk Committee is responsible for performing the duties set out in this Charter to enable the Board to fulfil its oversight responsibilities in relation to the Group's:

- risk and compliance management policies and frameworks, ensuring that they remain appropriate to the size, business mix and complexity of the Group, and are consistent with the Group's business plan; and
- identification, assessment and management of risk (encompassing financial and non-financial risk) and compliance in accordance with the Group's risk and compliance management policies and frameworks.

Composition

The Risk Committee will be appointed by the Board and shall comprise not less than three directors. All members of the Risk Committee must be non-executive directors, and a majority of members must be independent.

Chairman

The Board shall appoint one of the Risk Committee members to serve as the Risk Committee Chairman. The Risk Committee Chairman shall be an independent director. The Risk Committee Chairman will not be the Chairman of the Board. The Risk Committee Chairman and membership will be confirmed annually.

Administrative Matters and Procedures

Meetings shall be held at a frequency determined by the Risk Committee but in any event not less than five times per year. Special meetings may be convened by the Risk Committee Chairman as required.

A quorum of any meeting will be two members or such other number determined by the Board. The agenda and supporting documentation will be circulated to the Risk Committee members in a reasonable period in advance of each meeting.

Board members, who are not Risk Committee members, will receive copies of papers and may attend meetings of the Risk Committee as observers.

Non-committee members may attend part or all of any meeting of the Risk Committee at the invitation of the Risk Committee Chairman. The Risk Committee Chairman will offer standing invitations to the Group CEO & Managing Director, the Chief Risk Officer, the External Auditor and the Executive General Manager Internal Audit. Specific invitations will be offered to other Group Executives to lead discussions in their areas of accountability where required.

The secretary of the Risk Committee will be the Company Secretary, or such other person as nominated by the Board. The secretary of the Risk Committee will circulate minutes to members of the Risk Committee and the Board as soon as practicable after each meeting.

The Risk Committee Chairman will provide the Chief Risk Officer with clear right of access to the Risk Committee and the Board.

Any time sensitive matters that may require engagement of the Risk Committee in between meetings should be raised by the Group CEO & Managing Director or the Group Chief Risk Officer with the Risk Committee Chairman. The Risk Committee Chairman will determine if a formal Board or Risk Committee meeting needs to be convened or how the Committee members will be otherwise informed. In addition, any Risk Committee members may raise a time sensitive matter directly with the Risk Committee Chairman outside of the scheduled meetings.

Reporting

The Risk Committee shall submit an update to the Board summarising the Risk Committee activities and detailing any approvals or recommendations after each committee meeting.

The Risk Committee shall submit an annual Letter of Representation to the Audit Committee confirming the status of material risk issues considered by the Committee that may be relevant to the annual Financial Statements.

Duties and Responsibilities

The Risk Committee shall:

- review and approve or recommend for approval by the Board the Group's Risk Management Strategies, the Enterprise Risk Management Framework and Group Policies, principles, limits, standards and guidelines in relation to specific categories of risk;

- oversee the performance of the Group against the Risk Management Strategies, management's implementation and operation of the Enterprise Risk Management Framework and adherence to internal risk and compliance management policies, principles, limits standards and guidelines;

- review and consider an independent report on the appropriateness, effectiveness and adequacy of the Group's Enterprise Risk Management Framework, against prudential requirements as required, or at least every three years;

- review and recommend for approval by the Board the Risk Appetite Statements for the Group and its Australian general insurance and banking entities, and thereafter oversee adherence of the Group to the approved Risk Appetite Statements;

- review and consider the Group's risk profile, including receiving reports from management on:

    - its assessment of the risks described in the Enterprise Risk Management Framework including key risk and compliance exposures and any actions being taken to ensure that the Group continues to operate within risk appetite or to bring risk levels back within the risk appetite set by the Board;

    - material matters that may impact risk and compliance exposures, and actions being taken to address these;

    - data from risk systems, demonstrating attention to core risk and compliance management practices, that encompasses risks, compliance obligations, controls, incidents and actions;

    - actions being taken to strengthen risk and compliance management practices, including the control environment;

    - key risk categories including Strategic Risks, People Risk and Technology Security Risk, and Aggregate Risk Exposures; and

    - actions to address significant risk incidents, compliance breaches and material deviations from the Enterprise Risk Management Framework, including "lessons learned" and thematic or systemic issues that require attention.

- oversee the Group's legal, regulatory and industry code compliance processes including compliance by subsidiary companies, and where considered necessary, commission and direct specific actions and assignment of responsibility to ensure compliance practices are adequate;

- oversee management's actions to address the risk and compliance implications of new and emerging risks, regulatory change, organisational change and major initiatives;

- oversee Management's approach to breach management and the fair and timely completion of material customer remediation programs across the Group;

- review and consider reports from internal and external audit that provide a third line of defence view of the risk and compliance activities of the Group;

- oversee management's assessment of risk culture and consider actions required to ensure a sound risk culture is maintained and make recommendations to the Board as required;

- review and approve or recommend to the Board for approval (or as per each Policy's stated Approval Body) any new, material variation in, or repeal of Group Policies;

- endorse, approve or review (as the Risk Committee considers appropriate) any transaction or other proposal that involves Group Executives exceeding limits detailed in Group Policies;

- review and approve any recommendations made by management in accordance with Delegations of Authority assigned to the Risk Committee under Group Policies (including for new products and platforms);

- review and recommend for approval by the Board the APRA Risk Management Declaration, Financial Services Council Statement of Compliance and any other statutory statements covering governance and risk management matters in accordance with regulatory requirements;

- review and approve the Intra-Group Transactions and Exposure Limits, and review and consider reports from management that monitor the exposures against the approved limits;

- review and consider the approach, objectives, timeframes, scenario considerations and outcomes for the Group capital stress testing and their application in setting the Group's risk appetite and capital targets;

- direct management (including the Chief Risk Officer) to prepare and present reports or updates on matters of relevance to the Risk Committee in fulfilling its role;

- constructively challenge management recommendations and actions with the objective of improving the Group's approach to risk and compliance management; and

- direct any special investigations deemed necessary and engage and consult independent experts where considered necessary or desirable to carry out its responsibilities and rely on the advice of such experts.

Other Responsibilities

The Risk Committee shall:

- in consultation with the Group CEO & Managing Director, provide prior endorsement for the appointment of (and thereafter monitor his/her performance and objective setting) and, if relevant, removal of the Group Chief Risk Officer;

- regularly review this Charter and its continuing adequacy, together with an evaluation of the Risk Committee's effectiveness and the extent to which the Risk Committee has met the requirements of the Charter. The Risk Committee shall, as required, recommend changes in the Charter to the Board for approval; and

- be available to meet regulators on request.

Interaction with the Board and Other Committees

The Chairman of the Risk Committee will periodically meet with the Chairman of the:

- Board;
- Customer Committee;
- Audit Committee;
- People & Remuneration Committee; and
- Other standing committees of the Board as appropriate

to consider and share key information identified by those committees.

Matters requiring the attention of the Board and other committees will be circulated to the appropriate committee by the secretary of the Risk Committee.

Function of Representative Parties

It is recognised that members of the Risk Committee are not full-time employees of the Group and generally do not represent themselves to be experts in the fields of risk management. As such, it is not the responsibility of the Risk Committee personally to conduct risk management reviews.

The Group Executives are responsible for identifying, assessing and managing risk within the Group's risk appetite and policy requirements and implementing systems to effectively manage compliance obligations. The Group Executives will provide regular updates to the Risk Committee on these activities, where appropriate, and will escalate issues to the Risk Committee for its review as and when appropriate.

The Chief Risk Officer is responsible for defining the risk management process and policy frameworks, providing challenge to the first line of defence on risk management activities, assessing risks and reporting to the Risk Committee. The Chief Risk Officer is responsible for the preparation and coordination of information provided to the Risk Committee, and in doing so may rely upon information contained within risk systems and reports prepared by management in accordance with the three lines of defence model as described in the Enterprise Risk Management Framework.

Internal Audit is responsible for independent assurance over the effectiveness of the systems of controls and the application of the Enterprise Risk Management Framework.

Rights of Access and Authority

Each member of the Risk Committee has rights of access to executives, risk and financial control employees, Appointed Actuaries, Internal Audit and External Audit without management present, and rights to seek explanations and additional information from both management and auditors, in order to fulfil their role and undertake their duties.

Schedule: Risk Committee Charter

Item 1: Name of Company

Suncorp Group Limited

Item 2: Name of Entities

SBGH Limited, Suncorp Insurance Holdings Limited, Suncorp Life Holdings Limited and all other controlled entities within the Suncorp Group except superannuation entities regulated by APRA.