CYBER AND TECHNOLOGY RISK COMMITTEE – TERMS OF REFERENCE

A. MANDATE

The Board of SBM Bank (Mauritius) Ltd (''Bank'' or "Company") has established the Cyber and Technology Risk Committee (''the Committee'') to provide oversight and strategic guidance on the Bank's cyber, digital, and technology agenda, and to assist the Board in assessing and monitoring the cyber, information and technology risk management.

B. COMPOSITION

The Board of the Bank must appoint a minimum of 3 (three) and a maximum of 7 (seven) directors to be members of the Committee. The Committee shall be composed of a majority of non-executive directors of the Board. The Chairperson of the Committee shall be an independent director.

At least two of the independent directors of the Committee shall have relevant experience in cyber/technology matters.

The Committee may, at its discretion, invite external advisers or subject matter experts to provide independent perspectives. Rotation of members shall be considered periodically to ensure independence and fresh perspectives.

C. SECRETARY

The Company Secretary or his/her nominee, shall act as Secretary of the Committee and ensure timely distribution of meeting materials and records.

D. QUORUM

The Quorum of the Committee shall be three (3) members.

E. RESPONSIBILITIES

The Committee is responsible for performing the duties set out below as well as any other duties that are otherwise applicable by law or regulations or delegated to the Committee by the Board.

The main duties of the Committee are to:

1. Cyber & Technology Strategy
- Review and recommend to the Board for approval, a comprehensive cyber and technology risk management strategy, framework and related policies.
- Periodically review the cyber and technology risk management strategy, framework and related policies and make recommendation to the Board in case of significant changes.
- Oversee the Bank's digital transformation and major technology initiatives, ensuring risk, resilience, and Return on Investment are balanced.

2. Risk Oversight & Monitoring
- Receive periodic reports from the Chief Risk Officer ("CRO") on the performance of the cyber and technology risk management framework, and overall status and effectiveness of the cyber and technology risk management framework, amongst others.
- Receive regular reports from the Chief Executive ("CE") and the Chief Information & Digital Officer ("CIDO") on the implementation and performance of the cyber and technology risk management framework and strategy along with the execution of cyber/technology-related critical projects.
- Receive quarterly reports and from the Chief Information Security Officer ("CISO") on:
  a) the implementation of the cyber and technology risk management framework;
  b) the overall cyber and technology risk position of the Bank, including trends in key performance metrics, results of assessment of training and awareness programs, key developments in the threat landscape and key findings from testing exercises, audits and other reviews; and
  c) the effective implementation of and compliance to the Bank's cyber and technology risk policies.
- Receive assurance from the Chief Executive that the relevant functions with cyber and technology related responsibilities (including the first and second lines of defense) is properly structured and equipped in terms of resources, budget, training and solutions to adequately carry out their activities.

3. Resilience & Crisis Preparedness
- Receive assurance from the Chief Executive and CISO that an adequate crisis management response plans are in place and that simulation exercises are conducted on a regular basis.

4. Compliance & Governance
- Oversee compliance with the Mauritius Data Protection Act, GDPR, Bank of Mauritius guidelines, and other applicable laws/regulations; and
- Promote responsible adoption of emerging technologies.

5. People & Culture
- Mandate the Senior Management to ensure adequate resources, budget, skills, and trainings are allocated to technology and cyber risk management;
- Require Senior Management to ensure that all personnel of the Bank attend all mandatory cyber, information and technology risk trainings periodically; and
- Foster a culture of cyber awareness, ethical technology adoption, and compliance with data protection and privacy regulations.

F. REPORTING AND ACCOUNTABILITY

The Committee will report to the Board in a timely manner on all significant cyber, digital and technology related matters it has addressed, such matters that could have a major impact on the Bank's cyber, digital and technology function and to such other related matters that are within its responsibilities.

The chairperson (or, in his/her absence, an alternate member) of the Committee shall attend the annual meeting to answer questions concerning matters falling within the ambit of the Committee.

G. AUTHORITY

The Committee has authority to conduct any matters under the scope of its responsibility.

The Committee, in carrying out its tasks under these Terms of Reference, may have access to any information necessary to discharge its duties, commission independent reviews, penetration tests, or forensic investigations as it considers necessary and recommend to the Board suspension of critical technology initiatives if risk thresholds are breached.

H. REVIEW

The Committee will review the Terms of Reference at least annually and submit it to the Board for approval together with such amendments as it deems necessary and appropriate in the light of the Bank's requirements as well as any legal and regulatory developments.

I. ASSESSMENT

At least annually, the Board, acting through the Committee, will assess its effectiveness in fulfilling its responsibilities and duties as set out in the Terms of Reference and in a manner consistent with the Strategic Guidelines adopted by the Board.

J. CHAIR

Each year, the Board on the recommendation of the Committee will appoint one member to be its Chair. If, in any year, the Board does not appoint a Chair, the incumbent Chair will continue in office until a successor is appointed.

K. MEETINGS

1. Frequency

- The Committee shall meet on a quarterly basis, however ad-hoc meetings may also be convened by the Chair, or any member of the Committee or the Chief Executive.
- At least one joint session annually shall be held with the Board Risk Committee and/or Audit Committee.
- Annual deep-dive sessions shall be organised on emerging technology and cyber risks (e.g., AI, quantum computing, geopolitical threats).
- The Chairperson may, at her/his discretion, invite other executives to attend and to be heard at meetings of the Committee.

2. Notice

- Meetings of the Committee shall be convened by the Secretary of the Committee at the request of the Chairperson or any of its members.
- Notice of each meeting confirming the venue, time and date together with an agenda of items to be discussed and supporting papers, shall be forwarded to each member of the committee, and any other person required to attend, no later than five working days before the date of the meeting or as per timeline agreed with the Chairperson.

3. Minutes

- The minutes of all meetings of the Committee, or summaries thereof, shall be submitted to the Board at the immediate quarterly Board meeting, the agenda for each such board meeting shall provide an opportunity for the Chairperson of the Committee to report orally on any matters of importance as well as on the Committee's findings and shall recommend actions.

L. VOTING

Matters are debated and decisions shall be taken by Majority of Votes of the Members present at a meeting and in the case of an equality of votes, the Chairperson of the meeting shall have a second or casting vote. Any dissent from the Member/s should be minuted.

In the event, a Member is conflicted on a proposal, he/she should declare his/her interests and abstain from the deliberation and decision-making on the proposal.

M. REMUNERATION

Having regard to the functions performed by the members of the Committee in addition to their functions as directors in relation to the activities of the Committee, the Members may be paid such special remuneration in respect of their appointment as shall be fixed by the Board. Such special remuneration shall be in addition to the annual fees payable to directors.

N. REMOVAL AND VACANCIES

Any member of the Committee may be removed and replaced at any time by the Board and will automatically cease to be a member as soon as he or she ceases to be a Director. The Board will fill vacancies on the Committee by appointment among qualified members of the Board.