Cyber & Technology Committee - Terms of Reference

The Terms of Reference of the Cyber & Technology Committee (the "Committee") was approved by the Board on 26 August 2025.

The Committee shall assist the Board in reviewing, assessing and monitoring all Information Technology, Cyber Security and digitalisation related matters. This includes providing oversight of the Bank's technology strategy, digital transformation, and major technology investments, monitoring and advising on cybersecurity risk management and regulatory compliance and ensuring alignment between business strategy, IT strategy, and risk appetite.

1. Membership/Composition

1.1. The Committee shall consist of a minimum of three (3) members and a maximum of five (5) members provided that at least two (2) of the members shall be non-executive directors with relevant experience in cyber / technology related matters.

1.2. The CEO shall also be a member of the Committee.

1.3. **Chairperson** - The Chairperson should be a non-executive director but preferable an Independent non-executive Director. The Chairperson of the Board may be a member of the Committee but not its Chairperson.

1.4. In the absence of the Chairperson, the remaining members present shall elect one of themselves to chair the meeting.

2. Meetings

2.1. Frequency of Meetings - At least once every quarter or more frequently as circumstances require.

2.2. Meetings of the Committee shall be convened by the Secretary, in his absence by his Deputy or any authorised officer, of the Committee at the request of the Chairperson or by any of its members.

2.3. The notice of each meeting of the Committee confirming the venue, time and date and enclosing an agenda of items to be discussed shall, other than under exceptional circumstances, be forwarded to each member of the Committee at his known registered address or electronic communication/email or Board Vantage.

2.4. Agenda, Committee documents and a prior written notice of at least five (5) business days shall be sent to each member for any meeting of the Committee. In case of urgent matters, a prior notice of two (2) business days shall be given.

2.5. The requirements provided above may be varied subject to the written consent of all members.

2.6. Deliberations by way of circularisation assented to by all members then entitled to receive notice of a meeting of the Committee, is as valid and effective as if it had been passed at a meeting of the Committee duly convened and held.

2.7. Proceedings of the Committee shall be reported periodically to the Board of Directors preferably on a quarter basis.

2.8. Only members of the Committee shall have the right to attend the Committee's meetings however, the Committee may invite non-members and reporting officers.

2.9. Members of the Committee are entitled to vote and each member shall have one vote. The Chairperson shall not have a casting vote. The majority of votes shall decide a matter, and in the event of a deadlock, the matter shall be referred to the Board for resolution.

3. Secretary

3.1. The Company Secretary shall act as the Secretary of the Committee and will ensure that the Committee receives information and papers in a timely manner to enable full and proper consideration to be given to the issues.

4. Quorum

4.1. The quorum for any meeting shall be a majority of its members.

5. Minutes of Meetings

5.1. The Secretary shall minute the proceedings and decisions of all meetings of the Committee, including recording the names of those present and in attendance.

5.2. Draft minutes of Committee meetings shall be circulated to all members of the Committee, within fifteen (15) business days of the Meeting, unless circumstances dictate otherwise under which the Company Secretary shall then inform the members accordingly.

6. Role & Responsibilities

The duties of the Committee should review and assess, where relevant, and make its recommendations to other Committees / the Board on the following matters, *inter alia:* -

6.1. Strategy and policies

6.1.1. Strategies and framework related to Cyber and Technology including e-banking products and services;

6.1.2. Relevant Cyber and Technology policies, implementation of Technology and digitalisation initiatives/projects as approved and aligned with the overall business strategy;

6.1.3. Cyber and technology security awareness and training program for staff, directors and senior management including monitoring of the effectiveness of such programs through periodic testing, feedback, and reporting of awareness levels and user behavior metrics (e.g., phishing simulations);

6.1.4. Operating models of Cyber & Technology areas, including Responsibility, Accountability, Consulted & Informed [RACI] Matrix;

6.1.5. Architecture blueprints for enterprise, business, technical and so on, as per mapping to organizational-wide processes;

6.1.6. Any relevant proposals, updated policies, standards, procedures and framework related to Cyber and Technology Security blue print in line with the security strategies of the Bank.

6.1.7. Ensure the formal adoption, implementation and annual review of a Cybersecurity Governance Framework consistent with the Bank of Mauritius Cybersecurity Guideline.

6.2. Risks

6.2.1. Receive reports on material cyber and technology incidents, on the evolution of the threat landscape and on the status and effectiveness of the cyber and technology risk management framework;

6.2.2. Assessment of cyber and technology investments for sustaining the bank's growth considering proper balance of costs, risks and benefits;

6.2.3. Review, assess and recommend to the Audit Committee the Internal Audit's IT Annual Audit Plan and the corresponding Risk assessment;

6.2.4. Assessment, control, manage and mitigate Information, Cyber and technology risks as identified during audit process and to liaise with the Risk Committee accordingly;

6.2.5. Create awareness about exposure towards IT and Cyber Technology risks and controls, effectiveness of management's monitoring of IT and Cyber Technology risks through oversight over the proceedings of the Information Security Management Committee;

6.2.6. Ensure that appropriate business continuity arrangements / measures are in place;

6.2.7. Monitoring of the bank's information management and data governance framework and systems including those relating to compliance with the General Data Protection Regulations (and any analogous legislation).

6.2.8. Ensure appropriate IT Risk Assessment is conducted on regular basis and Risk Register is up to date at all times.

6.2.9. Ensure vulnerabilities assessment and penetration testing is performed as and when needed and follow up on timely execution of remediation plan.

6.2.10. Ensure that a Cyber Incident Response Plan (CIRP) is established, regularly tested, and updated, and that material cybersecurity incidents are reported to the Bank of Mauritius within the regulatory timelines.

6.2.11. Review post-incident reports and ensure lessons learned are implemented to improve resilience.

6.2.12. Ensure that a data classification framework is implemented, sensitive data is identified, and appropriate controls (encryption, access controls, etc.) are in place based on data sensitivity.

6.2.13. Oversee the conduct of periodic cyber resilience assessments, such as red teaming, simulated phishing, and tabletop exercises, to validate response capabilities.

6.2.14. Oversee the assessment and mitigation of cybersecurity risks in the Bank's supply chain, including vendors, partners and other interconnected entities.

6.2.15. Ensure that cybersecurity practices, controls and frameworks are reviewed periodically to remain aligned with applicable regulatory requirements including the Bank of Mauritius Cybersecurity Guideline.

6.3. Resources

6.3.1. Appointment of any such person (employee, consultant or advisor) to undertake any specific projects or assignments in relation to the Bank's technology, security or digitalisation initiatives/projects, and to review the progress of such engagements, for escalation from the relevant management committees.

6.3.2. Review the on-going appropriateness and relevance of the bank's policy for the allocation of resources required to deliver both the short-term and long-term information technology strategies;

6.3.3. Review and classify all cyber and technology outsourcing related-activities and projects as well as monitoring closely the performance of service providers, ensuring they meet the Bank's cybersecurity requirements, and that appropriate Service Level Agreements (SLAs) and independent assurance reports (e.g. SOC 2, ISO 27001) are obtained and reviewed periodically.

6.3.4. IT organizational structure complements the business model and its direction.

6.3.5. Oversee the cyber and technology landscape and the adequacy of human and other resources.

6.4. Performance and value

6.4.1. Ensure that Management has implemented relevant processes and practices that ensure that the IT services deliver value to the business;

6.4.2. Assess whether priorities set by management is as per overall strategy and business short term, mid-term and long-term goals

6.4.3. Assess senior management's performance in implementing IT strategies, policies, projects and contribution of Cyber Technology to businesses.

6.4.4. Review and approve the Key Performance Indicators for Cyber and Technology teams as per established strategy

6.5. Budgets

6.5.1. Review and monitoring of the cyber and technology OPEX and CAPEX budgets vs actual;

6.5.2. Assessment and recommend proposed cyber and technology OPEX and CAPEX budgets.

6.6. Other

6.6.1. To undertake such other duties and responsibilities as determined by the Board of Directors of the bank for this Committee from time to time.

7. Reporting Responsibilities

7.1. The Chairperson shall report to the Board on its deliberations after each meeting on all significant matters within its duties and responsibilities.

7.2. The Committee shall make relevant recommendations to the Board it deems appropriate on any Cyber and IT-related areas within its remit where action or improvement is needed.

7.3. Receives and reviews regular cyber risk dashboards with key performance indicators (KPIs) and key risk indicators (KRIs), and reports material trends or deviations to the Board.

8. Other matters

8.1. The Committee is authorised to seek any information from any officer or employee all of whom are directed to co-operate with any request made by the Committee.

8.2. The Committee shall have access to outside or other independent professional advice as it considers necessary to carry out its duties at the Bank's expense within any reasonable budgetary guidelines as indicated by the Board.

8.3. Regular training on IT, Cyber Technology, Cyber Security, IT risks and any other areas should be provided to the members for continuous development. The Committee may decide on the focus areas.

8.4. The Committee shall have access to sufficient resources in order to carry out its duties, including full access to the bank's secretariat for assistance as required.

8.5. The Committee shall give due consideration to laws, regulations and any published guidelines or recommendations.

8.6. The Committee shall arrange for periodic reviews of its own performance and review its terms of reference on an annual basis to ensure it is operating at maximum effectiveness and recommend any changes it considers necessary to the Board for approval.