



SUCCESS BEYOND NUMBERS

Cyber and Technology Risk Committee Charter

Contents

1. Objectives	2
2. Composition.....	2
3. Meetings	2
4. Role and responsibilities	3
5. Other Provisions	5

1. Objectives

The Cyber and Technology Risk Committee (“CTRC”), a joint Committee of the boards of directors of The Mauritius Commercial Bank Ltd and MCB Group Limited, hereafter designated as “the Boards”, shall assist the Boards in defining risk strategies, in assessing and monitoring the cyber, information and technology risk management of all the subsidiaries of, and including, MCB Group Limited (all of which will be collectively referred to as “MCB” in the rest of this document). The CTRC shall also advise the Boards on cyber, information and technology risk issues and shall monitor the associated risk levels and postures against the set risk appetites.

This Charter is posted on the organisation’s website.

2. Composition

- 2.1. The CTRC shall consist of a minimum of six members, of whom two independent directors shall be from MCB Group Limited and two independent directors shall be from The Mauritius Commercial Bank Ltd.
- 2.2. Two Chairpersons will be designated to co-chair the CTRC with one Chairperson appointed by the board of directors of MCB Group Limited and the other appointed by the board of directors of The Mauritius Commercial Bank Ltd.
- 2.3. The Chairpersons and the members of the CTRC shall be appointed by the Boards on the respective recommendation of the Corporate Governance and Sustainability Committee (“CGSC”) of MCB Group Limited and of the Nomination and Remuneration Committee (“NRC”) of The Mauritius Commercial Bank Ltd.
- 2.4. The Chairpersons shall both be independent directors.
- 2.5. At least two of the independent directors of the CTRC shall have relevant experience in cyber/technology matters.
- 2.6. The Boards may at any time replace member/s of the CTRC and fill any vacancy/ies.

3. Meetings

- 3.1. Meetings shall be held quarterly, or more frequently as circumstances require.
- 3.2. The Chairpersons shall convene a meeting upon the request of any CTRC member who considers it necessary.
- 3.3. The quorum for the CTRC shall be four directors, a majority of whom being independent directors. In case the quorum cannot be fulfilled, the Chairpersons of the CTRC may appoint another independent non-executive director in replacement.

- 3.4. Any Chairpersons of the CTRC may designate an alternate in case of absence. In case of absence of any of or both Chairpersons and where no alternate has been designated, either the NRC and/or the CGSC or the Chairpersons of the Boards shall appoint an independent non-executive director to chair the meeting.
- 3.5. The Secretary of the CTRC shall keep appropriate records of all meetings of the Committee with minutes of proceedings. The Secretary shall circulate minutes of any meeting of the Committee to all members of the Committee.
- 3.6. The Group Chief Risk Officer of MCB (“CRO”) and the Head of Enterprise Risk of the Mauritius Commercial Bank Ltd (reporting to the CRO, in the second line of defense and overseeing the cyber and information security activities and initiatives) shall report to the CTRC and will be called upon, at each CTRC session, to present on any topics covered in the CTRC’s roles and responsibilities. They shall also present and report on any other important matters relevant to the areas of responsibility of the CTRC.
- 3.7. The CTRC may request any officer or employee to attend any meeting and provide relevant information as necessary.
- 3.8. All decisions of the CTRC shall be made unanimously.

4. Role and responsibilities

- 4.1. The duties and responsibilities of the members of the CTRC shall be in addition to those set out for a member of the Boards.
- 4.2. The principal duties of the CTRC shall consist in reviewing and recommending to the Boards for approval of a comprehensive cyber, information and technology risk management strategy and framework. The CTRC shall ensure that these documents are aligned with MCB’s strategy and are maintained according to the current regulatory and threat landscape.

To achieve this objective, the CTRC shall perform the following tasks:

4.2.1. Strategies

The CTRC will review MCB’s cyber resilience strategy and all associated frameworks and upon validation, will ensure the Boards’ approval of these documents. Additionally, the CTRC will regularly review these documents and submit them for Boards’ approval in case of major changes.

4.2.2. Cyber, information and technology risk appetite:

The CTRC will review and validate the MCB’s cyber, information and technology risk appetite framework and upon validation will submit it to the Boards for approval and will enforce compliance, throughout MCB, with the requirements of the cyber, information and technology risk appetite framework and will ensure that it is adjusted based on the evolving threat landscape.

4.2.3. Policies:

The CTRC will regularly review and validate all cyber, information and technology risk policies and, upon validation, will submit these to the Boards for approval.

4.2.4. Reports:

The CTRC will ensure that it receives regular transparent reports on cyber, information and technology incidents, on the evolution of the cyber threat landscape, on the findings of audit exercises, on the results of vulnerability assessments, on the results of penetration testing, on the results of red/purple team exercises, on the results of controlled social engineering attacks, on the status of cyber security compliance initiatives, on the implementation progress of cyber, information and technology risk initiatives/solutions and on the overall status and effectiveness of the cyber, information and technology risk management framework.

4.2.5. Cyber, information and technology risk culture and training:

The CTRC will ensure a strong cyber, information and technology risk culture across the organization and will ensure adherence of all personnel with the requirements of the cyber risk culture initiatives.

The CTRC will mandate senior management of all subsidiaries of MCB to ensure that:

- all personnel of MCB attend all mandatory cyber, information and technology risk training,
- the resilience level of MCB, faced with a simulated social engineering attack, remains in line with similar international industry standards, and
- adequate crisis management response plans are in place and that simulation exercises are conducted on a regular basis.

4.2.6. Cyber, information and technology risk maturity:

The CTRC will ensure that all subsidiaries of MCB have adequate cyber, information and technology risk controls in line with their associated inherent risk levels.

4.2.7. Resource allocation:

The CTRC will ensure that both the first and second lines of defense (i.e. the Information Security BU and Cyber and Information Security BU respectively) as well as the relevant sections of Technology SBU are properly structured and equipped in terms of resources, budget, training and solutions to adequately carry out their activities.

4.2.8. Independence:

The CTRC will ensure that both first and second lines of defense (i.e. the Information Security BU and Cyber and Information Security BU respectively) always remain independent from technical or information technology operations, with the second line of defense reporting to the CRO.

4.2.9. Compliance with laws and regulations:

The CTRC will ensure compliance with all laws and regulations relevant to cyber, information and technology risks, including, but not limited to, the Data Protection Act (2017) and the Guideline on Cyber and Technology Risk Management issued by the Bank of Mauritius.

5. Other Provisions

5.1. Professional advice

The Boards have an agreed procedure whereby directors can seek independent professional advice, should the need arise. The professional services procured shall be at the Company's expense and prior approval of both Chairpersons is required.

5.2. Access to information

The CTRC shall have access to sufficient resources to carry out its duties, including access to the Company Secretariat of MCB for assistance as required.

5.3. Reporting

The Chairpersons of the CTRC shall report formally to their respective Boards in a timely manner on its proceedings after each meeting. A report will be made at least quarterly when the Boards examine the financial statements for approval and release.

5.4. Review of Charter

The Committee shall review this Charter at least every two years and recommend any amendments to the Board for approval. The Charter shall be updated promptly to reflect material changes in applicable laws, regulations or Bank of Mauritius guidelines.