CIMB Group Holdings Berhad

TERMS OF REFERENCE OF BOARD RISK AND COMPLIANCE COMMITTEE

---

1. OBJECTIVE

The primary objective of the Board Risk and Compliance Committee (Committee/BRCC) is to assist the Board of CIMB Group Holdings Berhad (CIMB) in discharging its responsibilities including providing oversight and advice to the Board and Management on:

- Supervising Management's execution of CIMB's internal control frameworks and related policies.
- Ensuring Management adheres to the risk governance expectations as outlined in the Group Policy Management Framework.
- Monitoring Management's implementation of compliance and risk management practices.

2. SIZE AND COMPOSITION

The Committee shall:

(a) have at least three (3) Directors,

(b) comprise only Non-Executive Directors, majority of which shall be Independent Directors,

(c) be chaired by an Independent Director who is not the Chairperson of the Board, and

(d) comprise Directors who possess the necessary skills, knowledge, and experience that align with the Committee's responsibilities.

3. SECRETARY

3.1. The Company Secretary and/or his/her nominee(s) shall act as Secretary to the Committee.

3.2. Minutes of Committee meetings shall be kept and circulated to all members of the Committee. The Committee shall brief the Board on key matters and concerns discussed, and where appropriate, provide relevant recommendations for the Board's consideration.

4. MEETINGS

4.1. The Committee shall meet at least four (4) times a year. Additional meetings may be called at the discretion of the Chairperson.

4.2. At least two-thirds (2/3) of the number of Directors must be present to form a quorum, majority of whom shall be Independent Directors.

4.3. In the event the Chairperson is not present within fifteen (15) minutes after the time appointed for the meeting, is unwilling to act or unable to attend the meeting, the remaining Directors shall elect an Independent Director among themselves to chair the meeting.

4.4. The Committee may invite any other Director, Senior Management, employees and professional advisors to be in attendance during meetings to assist in its deliberations.

4.5. Meetings may be conducted physically or by way of telepresence, teleconference, or other communication facilities available which would facilitate participation by the Directors, provided such facilities enable Directors to communicate with each other and to vote at such meetings. Participation of Directors at meetings by way of telepresence, teleconference or other facilities shall be treated as present in person and shall be counted towards the quorum for the meeting.

5. RESOLUTION PASSED/APPROVED

5.1. Subject to Clause 5.3, resolutions proposed at meetings or by circular shall be approved/passed by a simple majority of the members, each member having one vote.

5.2. Circular Resolutions which have been passed since the last Committee meeting shall be circulated for notation at the next meeting.

5.3. A Committee member who has, directly or indirectly, an interest in a material transaction or material arrangement shall not be present at the Committee meeting where the said matter is being deliberated by the Committee.

6. AUTHORITY

6.1. The Committee has delegated authority from the Board of CIMB to discharge its duties and responsibilities as set out in this Terms of Reference.

6.2. The Committee is authorised by the Board to obtain resources which it requires, including but not limited to, obtaining expert advice, both internal and external, upon approval by the Board and at CIMB's expense, as well as to have full and unrestricted access to information to enable the Committee to fulfill its objectives and responsibilities.

6.3. The Committee is vested with such power and authority, specific or general, as may from time to time be conferred upon by the Board of CIMB.

6.4. The Board remains fully accountable for any authority delegated to the Committee.

7. DUTIES AND RESPONSIBILITIES

The scope of the Committee's duties and responsibilities shall include the following:

7.1. Group Risk

(a) **Risk and Compliance Culture**

(i) To ensure a proactive risk management culture is implemented so that risk management processes and controls are applied and embedded in the day-to-day business and operational activities.

(ii) To ensure a framework is in place to facilitate the right compliance culture in the day-to-day business and operational activities.

(iii) To ensure Management provides guidance and support with regards to the Group's compliance efforts in the implementation of a proactive compliance risk management culture.

(b) **Recovery and Contingency Planning**

(i) To provide oversight and to review the recovery activities (i.e., development, maintenance, implementation of the recovery plan etc.) including recommending CIMB's Recovery Plan for approval by the respective Boards of CIMB Bank Berhad (CIMB Bank), CIMB Islamic Bank Berhad (CIMB Islamic Bank) and CIMB Investment Bank Berhad (CIMB Investment Bank).

(ii) To approve CIMB's contingency plan for dealing with various extreme internal/external events and disasters.

(c) **Risk Appetite**

(i) To determine the Group's Risk Appetite and Risk Posture taking into consideration the budget, business plans and expected macroeconomic conditions.

(ii) To ensure effective implementation of the Risk Appetite and Risk Posture by:

- approving changes to the Risk Appetite and Risk Posture throughout the year based on the macroeconomic environment, regulatory landscape, the Group's liquidity and capital profile, etc.;
- providing oversight on the compliance of approved Risk Appetite (via a Risk Appetite dashboard style format) and Risk Posture which are reported monthly/ quarterly respectively; and

- being apprised of action plans in cases where there is non-compliance with the Risk Appetite in accordance with approved policies and procedures.

(iii) To approve the annual Risk Appetite Statement.

(d) **Internal Capital Adequacy Assessment Process (ICAAP)**

(i) To review and assess adequacy of capital management framework and policies in line with capital strategy and regulatory requirements.

(ii) To ensure risk and capital management framework and policies are operating effectively and complied with.

(iii) To provide oversight on the risk and capital positions of the Group which are reported on a quarterly basis.

(iv) To approve the ICAAP of the Group annually by:

- ensuring that all relevant risks have been captured and the Group has sufficient capital resources in place;
- ensuring that the impact of any material event has been incorporated and, where appropriate, being apprised of the suitability of the risk assessment; and
- To oversee the overall stress testing programme, including climate risk stress testing, which encompasses providing strategic input into scenario development and approving the resulting stress test outcomes.

(e) **Risk Management Frameworks, Policies and Disclosures**

(i) To approve all disclosures and the corresponding Frameworks and Policies on disclosures, as well as the internal controls over the disclosure process in line with regulatory requirements.

(f) **Risk Identification and Measurement**

(i) To ensure infrastructure, resources and systems and other capabilities are in place for risk management and are adequate to maintain a satisfactory level of risk management and discipline.

(g) **Oversight on Technology Risks**

(i) To provide overall oversight on technological risks including ex-ante risk assessment on e-banking services.

(ii) To be regularly apprised by the Group Chief Information Security Officer (GCISO), who is accountable for the overall technology-related risks, and by the Group Chief Technology Officer (GCTO), who is accountable for the management, delivery and operations of IT services.

(h) **Third-Party Risk Management**

(i) To approve and be notified on Third-Party Arrangements, where required, in accordance with the Third-Party Risk Management Framework Approval Authority.

(ii) To have oversight over material adverse developments, any material non-compliance with the terms of agreement and any breach of legal and regulatory requirements by the Third-Party reported by Business Units/Business Enablers to Group Operational and Resiliency Risk Committee (GORRC) and Group Risk & Compliance Committee (GRCC).

(i) **Integrity and Governance**

(i) To review and recommend the Management's proposal on the Group Integrity & Governance Framework to the Board of CIMB.

(ii) To review and approve the amendments/changes to the Group Integrity & Governance Framework.

(iii) To oversee the functions of and review the report from the Integrity & Governance Unit (IGU) as set out in the Group Integrity & Governance Framework. The reporting by IGU shall include matters arising from the Group Anti-Bribery and Corruption Policy, Group Whistleblowing Policy, Group Code of Ethics & Conduct, and other related CIMB's Policies.

(iv) To assess and recommend to the Board the appointment of the Chief Integrity and Governance Officer (CIGO).

(v) To be apprised by the CIGO, on a quarterly basis or as and when required by the Board, on matters involving integrity, corruption, and abuse of power pursuant to the Group Integrity & Governance Framework.

(j) **Engagement with Group Chief Risk Officer**

(i) To be actively engaged and/or apprised by the Group Chief Risk Officer (GCRO) on all risk management issues and initiatives.

(ii) To review and recommend a key performance indicator (KPI) scorecard for the GCRO that incorporates the establishment of appropriate performance targets, parameters, and benchmarks at the beginning of each financial year.

(iii) To conduct annual assessment on the performance and effectiveness of the GCRO.

(k) **Other Matters**

(i) To approve contingency plan for dealing with various extreme internal/external events and disasters.

(ii) To be apprised of other risk and compliance related issues.

7.2. **Group Compliance**

(a) **Compliance Framework**

(i) To review and assess compliance and Anti-Money Laundering/ Counter Financing Terrorism (AML/CFT) risk issues and ensure such issues are resolved effectively and expeditiously.

(ii) To approve compliance and AML/CFT framework/ policies and material amendments to compliance and AML/CFT risk framework/ policies.

(iii) To evaluate the effectiveness of the compliance functions and overall management of compliance and AML/CFT risk.

(iv) To accord high attention and strengthen compliance functions, resources and infrastructure.

(b) **AML/CFT Risk Appetite**

(i) To determine the Group's AML Risk Appetite which includes sanctions risks by defining the terms and the risks that are acceptable to the Group. The AML Risk Appetite should be developed by considering the risks around Customers, Products, Channels and Geographies, as well as the types of businesses the Group can and cannot accept.

(c) **Compliance and AML/CFT Strategy**

(i) To review the compliance and AML/CFT strategy of the organisation; and

(ii) To define the compliance and AML/CFT risk management objectives across business lines.

(d) **Engagement with Group Chief Compliance Officer**

(i) To be regularly apprised by the Group Chief Compliance Officer (GCCO) on all compliance risk management issues and initiatives as well as regulatory developments.

(ii) To review and recommend a key performance indicator (KPI) scorecard for the GCCO that incorporates the establishment of appropriate performance targets, parameters, and benchmarks at the beginning of each financial year.

(iii) To conduct annual assessment on the performance and effectiveness of the GCCO.

8. DELEGATION OF RESPONSIBILITIES

8.1. The Committee may delegate relevant responsibilities to any appropriate Group-wide Management Committees, as it sees fit, to undertake or implement actions that have been approved or endorsed by the Committee.

8.2. Where the Committee has delegated such responsibilities, the Committee remains responsible for the exercise of the said delegation to those relevant Group-wide Management Committees.

8.3. The Committee further delegates the oversight of all risk-related matters undertaken by the Group's banking businesses to the Banking Group BRCC of the following subsidiaries:

(i) CIMB Bank;
(ii) CIMB Islamic Bank; and
(iii) CIMB Investment Bank.

The Banking Group BRCC operates within clearly defined roles and responsibilities as set out in its Terms of Reference.

9. ANNUAL PERFORMANCE ASSESSMENT

The Board shall review the composition and performance of the Committee and each of its members annually to determine the effectiveness of the Committee and its members in undertaking its duties and responsibilities as set out in this Terms of Reference.

10. REVIEW OF TERMS OF REFERENCE

This Terms of Reference shall be reviewed periodically to ensure it remains relevant and applicable. Any proposed revision or amendment to this Terms of Reference by the Committee shall be submitted to the Board for approval. Once approved by the Board, the revision or amendment shall be incorporated into this Terms of Reference and deemed officially adopted.