Updated as at 12 December 2024

TERMS OF REFERENCE OF THE BOARD RISK AND COMPLIANCE COMMITTEE OF CIMB GROUP HOLDINGS BERHAD

Objective

- To provide oversight and advice to the CIMB Group Holdings Berhad ("the Group") Board and Management in respect of all risks undertaken by the Group and future risk strategy, including determination of Risk Appetite.
- To provide oversight and advice to the Board and Management in respect of the management of compliance risk.

Composition

The Board Risk and Compliance Committee ("BRCC") should comprise only non-executive directors with at least three members. The BRCC should be chaired by an Independent Director.

The Company Secretary of CIMB shall act as Secretary to BRCC.

Quorum

The quorum for the BRCC is at least 50% of the members.

Frequency of Meetings

Meetings shall be held at least once every two months or as and when required.

Risk and Compliance Culture

- To ensure a proactive risk management culture so that risk management processes and controls are applied and embedded in the day-to-day business and operational activities.
- To ensure a framework is in place to facilitate the right compliance culture in the day-to-day business and operational activities.
- To ensure a proactive compliance risk management culture by providing guidance and support with regards to the Group's compliance efforts.

Oversight on IT Risks

- To provide overall oversight on IT risks including ex-ante risk assessment on e-banking services
- To be regularly apprised by the Group Chief Technology, who is accountable for the overall IT risks and security controls matters.

Recovery Planning

- To provide oversight and review the recovery activities (i.e., development, maintenance, implementation of the recovery plan etc.) including to approve the CIMB Group Holdings Berhad ("CIMBGH") Recovery Plan ("RCP") and recommend the RCP for approval by the

Boards of CIMB Bank Berhad, CIMB Islamic Bank Berhad and CIMB Investment Bank Berhad.

Third Party Risk Management

- In accordance to the Third Party Risk Management Framework Approval Authority, to approve and be notified on Third Party Arrangements, where required.
- Have oversight of material adverse developments, any material non-compliance to terms of agreement and any breach of legal and regulatory requirements by the Third Party that is reported by Business Units/Business Enablers to Group Operational and Resiliency Risk Committee (GORRC) and Group Risk & Compliance Committee (GRCC).

Roles and Responsibilities

GROUP RISK

1. Group Chief Risk Officer ("GCRO")
   - To be actively engaged or apprised by the GCRO, who reports directly to the BRCC, on all risk management issues and initiatives.
   - To set specific targets and KPIs for the GCRO and conduct annual assessment on the performance and effectiveness of the GCRO.

2. Risk Appetite
   - To determine the Group's Risk Appetite and Risk Posture taking into consideration the budget, business plans and expected macroeconomic conditions.
   - 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.
   - To approve the final annual Risk Appetite Statement.

3. Internal Capital Adequacy Assessment Process ("ICAAP")
   - To review and assess adequacy of capital management framework and policies in line with capital strategy and regulatory requirements.
   - To ensure risk and capital management framework and policies are operating effectively and complied with.
   - To provide oversight on the risk and capital positions of the Group which are reported on a quarterly basis.
   - To approve the ICAAP of the Group annually by:-
     - ensuring that all relevant risks to the Bank 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
     - being responsible for the overall stress test programme (including climate risk

stress testing).

4. Risk Management Policies and Disclosures
   - To approve all disclosures, disclosure policy and internal controls over the disclosure process in line with regulatory requirements.

5. Risk Identification and Measurement
   - To ensure infrastructure, resources, systems, and other capabilities are in place for risk management and are adequate to maintain a satisfactory level of risk management and discipline.

GROUP COMPLIANCE

1. Group Chief Compliance Officer ("GCCO")
   - To be regularly apprised by the GCCO, who reports directly to the BRCC on all compliance risk management issues and initiatives.
   - To set specific targets and KPIs for the GCCO and conduct annual assessment on the performance and effectiveness of the GCCO.

2. Compliance Framework
   - 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.
   - To approve compliance and AML/CFT framework/ policies and material amendments to compliance and AML/CFT risk framework/ policies.
   - To evaluate the effectiveness of the compliance functions and overall management of compliance and AML/CFT risk.
   - To accord high attention and strengthen compliance functions, resources and infrastructure.

3. AML/CFT Risk Appetite
   - 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.

4. Compliance and Anti-Money Laundering/ Counter Financing Terrorism ("AML/CFT") Strategy
   - To review the compliance and AML/CFT strategy of the organisation; and
   - To define the compliance and AML/CFT risk management objectives across business lines.

Other Matters

- To appoint external consultants, from time to time, to review and advise the BRCC on risk management and compliance matters;
- To approve the contingency plan for dealing with various extreme internal/external events and disasters; and
- To be apprised of other risk and compliance related issues.

Delegation Of Authority And Functions

The BRCC delegates the oversight in respect of all risks undertaken by the Group's banking businesses to BRCC of the following subsidiaries:

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

These Committees operate within clearly defined roles and responsibilities as set out in their respective terms of reference.