HONG LEONG FINANCIAL GROUP BERHAD

HONG LEONG INVESTMENT BANK BERHAD

HONG LEONG ASSURANCE BERHAD

HONG LEONG MSIG TAKAFUL BERHAD

GROUP BOARD INFORMATION AND TECHNOLOGY COMMITTEE (GBITC)

TERMS OF REFERENCE

CONSTITUTION

The Group Board Information and Technology Committee ("GBITC") is established to support the Boards of Hong Leong Financial Group Berhad ("HLFG"), Hong Leong Investment Bank Berhad ("HLIB"), Hong Leong Assurance Berhad ("HLA") and Hong Leong MSIG Takaful Berhad ("HLMT"), in discharging the following responsibilities:

1. Oversee technology and cyber security related matters.

2. Ensure that risks assessments undertaken in relation to material technology applications are robust and comprehensive.

3. Ensure that management meets the expectations on technology and cyber security risk management as set out in BNM's policy document on Risk Management in Technology.

4. Facilitate discussions amongst entities of the development in digital trends, to rationalise practices and policies and where possible, to seek consistent practices across entities.

For the purpose of this TOR:

- '**Boards**' means the Boards of (i) HLFG; (ii) HLIB; (iii) HLA; and (iv) HLMT.
- '**Companies**' and '**Company**' means (i) HLFG; (ii) HLIB; (iii) HLA; and (iv) HLMT.
- '**BARMC**' means Board Audit and Risk Management Committee.
- '**GBRMC**' means Group Board Risk Management Committee.

COMPOSITION

The GBITC shall:

(a) have at least three (3) directors;
(b) be chaired by an independent director;
(c) have membership representation from each of the Companies;
(d) comprise at least one member with the skills, knowledge and experience relevant to the responsibilities of this board committee.

SECRETARY

The Secretariat to the GBITC is the Company Secretary(ies) of HLFG.

TERMS OF REFERENCE

1. To review management's strategies relating to technology and cyber security and their alignment to the Companies' overall strategy, objectives and risk appetite.

2. To ensure that the Companies' technology risk appetite is aligned to Companies' overall risk appetite statement.

3. To review the adequacy of management's information technology and cyber security strategic plans over a three year period and periodically review these plans at least once every year.

4. To oversee management's implementation of sound and robust technology-related frameworks, encompassing technology risk management and cyber resilience.

5. To ensure that the Companies' technology-related frameworks encompassing technology risk management and cyber resilience, remains relevant on an ongoing basis.

6. To review the Companies' technology-related frameworks encompassing technology risk management and cyber resilience at least once every three years, for the Boards' affirmation.

7. To review management's reporting to the Boards on measures taken to:

   (a) Identify and examine technology risk (including cyber risk) faced by the Companies;
   (b) Ensure strategies are in place to safeguard the Companies against current and emerging technology and/or cyber risks;
   (c) Assess effectiveness of controls put in place to manage these risks; and
   (d) Conduct appropriate and timely closure of IT audit findings.

8. To review and ensure that management provides sufficient detailed information on key technology risk and critical technology operations to facilitate strategic decision-making. This includes reporting enterprise key risk indicators on the IT and cyber health posture.

9. To review and report to the Boards on emerging global technology trends and their potential application within the Companies, to either enhance the business operations, safeguard existing businesses or improve overall technology security.

10. To review post implementation reports of key technology projects to ensure that results are aligned to the risk posture stipulated in the initial project request.

11. To review and report to the Boards on the strategic benchmarking of technology performance against external peer groups from time to time.

12. To review the effectiveness of disaster recovery plans and disaster recovery testing to ensure high system resilience of technology systems, datacentres etc.

13. To review and ensure adequacy of cyber security investments and that its associated roadmap for implementation is acceptable.

14. Other technology and cyber security related matters as may be agreed by the Boards.

Group Governance

1. Noted that:

   (a) HLFG, as an apex entity has overall responsibility for ensuring the establishment and operation of a clear governance structure within its subsidiaries ("the Group").

   (b) HLFG Board's responsibility is to promote the adoption of sound corporate governance principles throughout the Group.

   (c) HLFG's IT related functions may propose objectives, strategies, plans, governance framework and policies for group-wide adoption and implementation.

   (d) The respective subsidiaries' board and senior management must validate that the objectives, strategies, plans, governance framework and policies set at HLFG level are fully consistent with the regulatory obligations and the prudential management of the subsidiary and ensure that entity specific issues are adequately addressed in the implementation of group-wide policies.

AUTHORITY

GBITC is authorised by the Boards to review any technology-related activities of the Companies within its terms of reference. It is authorised to seek any technology-related information it requires from any Director or member of management and all employees are directed to co-operate with any request made by the GBITC.

The GBITC is authorised by the Boards to obtain independent legal or other professional advice if it considers it necessary to perform the duties delegated by the Boards to this committee.

MEETINGS

The GBITC meets at least four (4) times a year and additional meetings may be called at any time as and when necessary.

The President and Chief Executive Officer, Group Managing Director/Chief Executive Officer, Chief Financial Officer, Chief Risk Officer, Chief Internal Auditor, Chief Compliance Officer, Chief Information Security Officer, Head of Group Operations and Technology, Chief IT Officer, other senior management and external auditors of HLFG and its subsidiaries may be invited to attend the GBITC meetings, whenever required.

Issues raised, as well as discussions, deliberations, decisions and conclusions made at the GBITC meetings are recorded in the minutes of the GBITC meetings. A GBITC member who has, directly or indirectly, an interest in a material transaction or material arrangement shall not be present at the GBITC meeting where the material transaction or material arrangement is being deliberated by the GBITC.

Two (2) members of the GBITC shall constitute a quorum.

After each GBITC meeting, the GBITC shall report and update the Boards on significant technology-related issues and concerns discussed during the GBITC meetings and where appropriate, make the necessary recommendations to the Boards for its deliberation and approval.

The minutes of each GBITC meeting shall be tabled to the Board of Directors of each Company.

REVISION OF THE TERMS OF REFERENCE

Any revision or amendment to the Terms of Reference, as proposed by the GBITC, shall be presented to the Boards for their approval. Upon the Boards' approval, the said revision or amendment shall form part of this Terms of Reference which shall be considered duly revised or amended.
