

HANG SENG BANK LIMITED

TERMS OF REFERENCE OF RISK COMMITTEE

1 Objective

1.1 The Board of Hang Seng Bank Limited (**the “Bank”**) has delegated to the Risk Committee (**the “Committee”**) oversight of risk-related matters impacting the Bank and its subsidiaries (**“HASE Group”**), including risk governance, internal control systems (other than internal controls over financial reporting) and culture-related matters.

2 Membership

2.1 The Committee shall comprise at least three members, all of whom shall be Non-executive Directors, with a majority (including the Chair) being Independent Non-executive Directors, or as otherwise required by local regulation.

2.2 The Chairman of the Committee shall be appointed by the Board from among the Independent Non-executive Directors.

2.3 The Chairman and each member of the Committee shall be appointed for an initial term until the conclusion of their current term of appointment as a Non-executive Director. Subsequent additional terms of appointment to the Committee may be made subject to review and approval by the Board.

2.4 The Secretary of the Committee shall be the Company Secretary or his/her nominee, who shall support the Chairman and Committee members in the operation of the Committee and its meetings.

2.5 Members of the Committee shall be appointed subject to endorsement by the Risk Committee of The Hongkong and Shanghai Banking Corporation Limited (**“HBAP”**).

2.6 At least one member of the Committee shall have recent and relevant accounting, banking or financial experience, or risk management expertise. When appointing Directors to the Committee, the Board shall have regard to the Committee collectively to have appropriate technical expertise and experience in risk disciplines relevant to the financial services sector.

3 Attendance

3.1 The Committee may invite any Director, executive, external auditor or other persons (including, but not limited to, the Chief Financial Officer, the Chief Risk Officer (**“CRO”**), the Head of Financial Crime Compliance, the Head of Regulatory Compliance and the Head of Audit) to attend any meeting(s) of the Committee as it may from time to time consider desirable to assist the Committee in the discharge of its responsibilities.

3.2 The Committee shall meet separately with the Chief Risk Officer, the Head of Audit and the external auditor at least twice each year without Management presence.

4 Meetings and Quorum

- 4.1 The Committee shall meet with such frequency and at such times as it may determine, subject to regulatory requirements.
- 4.2 The quorum for meetings is a majority of the members, including the Chairman (or his/her delegate from among the members).
- 4.3 Following each Committee meeting, the Chairman shall report at the next Board meeting on the Committee's proceedings. The minutes of the meeting shall be presented by the Committee Chairman at the first scheduled Board meeting after their preparation.
- 4.4 The Secretary of the Committee shall produce such papers and minutes of the Committee's meetings as are appropriate and distribute them to all members of the Committee.

5 Responsibilities of the Committee

Without limiting the generality of the Committee's objective, the Committee shall have the following non-executive responsibilities, powers, authorities and discretions:

5.1 Risk appetite

- 5.1.1 To satisfy itself that risk appetite informs HASE Group's strategy and business plans and that account has been taken of the macroeconomic and financial environment, drawing on financial stability assessments and other authoritative sources that may be relevant.
- 5.1.2 To advise the Board on risk appetite and risk tolerance related matters.
- 5.1.3 To review and recommend the Bank's Risk Appetite Statement at least annually to the Board for approval.
- 5.1.4 To receive reports where appropriate, to satisfy itself that the Bank's approach to the determination of its risk appetite is in line with regulatory requirements.

5.2 Risk-related matters

- 5.2.1 To oversee and advise the Board on risk related matters, including both financial and non-financial risks.
- 5.2.2 To review and provide independent challenge on risk management reports, including the Bank's enterprise risk reports to:
 - (a) assess the risk profile of the Bank and how the risks arising from the Bank's businesses are controlled, monitored and mitigated;
 - (b) focus on current and forward-looking risks to enable the Committee to assess the Bank's vulnerability and resiliency to potential risks;

- (c) review the effectiveness of the Bank's conduct framework designed to deliver fair outcomes for customers, preserve the orderly and transparent operation of financial markets, and protect the Bank against adverse outcomes (including reputational damage) to the Bank's financial and non-financial condition and prospects; and
 - (d) provide such additional assurance as the Board may require regarding the reliability of risk information submitted to it.
- 5.2.3 To require regular reports from the Management which :
- (a) enable the Committee to assess the risks involved in HASE Group's business and how they are controlled and monitored by Management;
 - (b) give clear, explicit and dedicated focus to current and forward-looking aspects of risk exposure which may require a complex assessment of HASE Group's vulnerability to hitherto unknown or unidentified risks; and
 - (c) enable the Committee to assess culture and changes thereof over time.
- 5.2.4 As applicable, to review and recommend the Bank's Internal Capital Adequacy Assessment Process ("**ICAAP**") to the Board for approval, and following that approval, to escalate any material issues relating to the capital component of the ICAAP to the Risk Committee of HBAP.
- 5.2.5 As applicable, to review and recommend the Bank's Individual Liquidity Adequacy Assessment Process ("**ILAAP**") to the Board for approval, and following that approval, to escalate any material issues raised during the Committee's ILAAP review, to the Risk Committee of HBAP.
- 5.2.6 To consider and advise the Board on the risks associated with proposed strategic acquisitions/disposals, focusing in particular on risk aspects and implications for the risk appetite and tolerance of the Bank.
- 5.2.7 To review and advise the Board and the Remuneration Committee on the Bank's alignment of remuneration with risk appetite.
- 5.2.8 To consider and advise the Board on the effectiveness of Management's policies for addressing risks relating to cyber security and information security.
- 5.2.9 To review and advise the Board on the effectiveness of Management's policies for addressing risks relating to the Bank's IT and operational resilience programmes.
- 5.2.10 To provide a forward-looking perspective to the Board on financial crime risk, including oversight of matters relating to:
- (a) financial crime risk and financial system abuse, including money laundering, sanctions, terrorist financing and proliferation financing;
 - (b) controls relating to bribery and corruption; and
 - (c) situations where the Bank may become exposed to financial crime and financial system abuse.

5.3 Stress testing

- 5.3.1 To review and satisfy itself that the Bank's stress testing framework, governance and related internal controls are robust.
- 5.3.2 To review and challenge the Management's interpretation of the scenario(s) prescribed by the regulator, including areas of judgement.
- 5.3.3 To review and challenge the results of, and supporting information for, enterprise-wide stress tests presented by the Management.
- 5.3.4 To review and approve, or recommend for Board approval, the Bank's final stress testing submissions to regulatory authorities.

5.4 Enterprise risk management framework and internal control systems

- 5.4.1 To annually review the Bank's enterprise risk management framework and satisfy itself that it is operating effectively.
- 5.4.2 To review the effectiveness of internal control systems (other than internal controls over financial reporting).
- 5.4.3 To review how effectively the Management is embedding and maintaining an effective risk management culture and a strong internal control environment designed to foster compliance with HSBC Group and the Bank's policies and regulatory compliance requirements.
- 5.4.4 In carrying out its oversight role, the Committee will consider any material findings from regulators relating to risk governance, conduct of business, risk assessment or management processes.

5.5 Culture

- 5.5.1 To advise and assist the Board's review of the effectiveness of culture enhancement initiatives so as to assess culture and changes thereof over time. In particular the Committee shall:
 - (a) at least annually, review, assess and approve the adequacy of the statement which sets out culture and behavioural standards;
 - (b) satisfy itself that the statement which sets out culture and behavioural standards is translated into policies and procedures, including, but not limited to, staff recruitment, training and incentive systems; and
 - (c) receive results from relevant assessment and feedback mechanisms at appropriate intervals (at least annually) for monitoring adherence to culture and behavioural standards.
- 5.5.2 To seek to embed and maintain throughout HASE Group a supportive culture in relation to the management of risk and maintenance of internal controls alongside prescribed rules and procedures.

5.6 Compliance

- 5.6.1 To approve the annual plan for the Compliance function and receive regular reports on progress against the plan and other matters relating to compliance risk and the Bank's relationship with its regulators.

5.7 Chief Risk Officer and risk management function

- 5.7.1 To monitor the effectiveness and independence (from the business) of the CRO and to review the composition and effectiveness of the risk management function including that it is of sufficient standing, independent of the business and adequately resourced.
- 5.7.2 To recommend to the Board the appointment or removal of the CRO.
- 5.7.3 To approve the annual plan for the Risk function and receive regular reports on progress against the plan.

5.8 Internal audit

- 5.8.1 To review reports from Internal Audit that provide assurance on the adequacy of internal control processes.
- 5.8.2 To request that the Management informs other Board committees (as applicable) on (a) material issues arising from or (b) shortcomings perceived in the scope or adequacy of, the work of Internal Audit relating to matters falling within the scope of such committees and that feedback is received from them.

5.9 External audit

- 5.9.1 To review any issue raised by the external auditor in respect of :
- (a) the audit of the Bank's annual report and accounts (and Management's response), or local equivalent, which relates to the management of risk or internal control systems (other than internal controls over financial reporting); or
 - (b) in connection with the external auditor's observations of the Bank's (i) regulatory standing and compliance or (ii) general competitive standing.

5.10 Annual report and accounts (or local equivalent)

- 5.10.1 Where applicable, to review and endorse the content of the risk committee report, risk disclosures or statements contained in the annual report and accounts, or local equivalent, relating to internal controls (other than internal controls over financial reporting), including the assessment of principal risks facing the Bank.

6 Other responsibilities

6.1 Certificates and assurance (escalation)

- 6.1.1 To provide half-yearly certificates to HBAP Risk Committee (in a form that is consistent with that required by the Group Risk Committee).

6.1.2 To take action and provide documentation or assurances as requested by HBAP Risk Committee including: providing copies of minutes, periodic certifications, adopting best practice, being forthcoming in sharing information, and interacting with its Chair on a regular basis.

6.1.3 The Committee shall, in carrying out the responsibilities set out in these terms of reference, discuss any concerns on potential risks to the Bank for escalation, if appropriate, to HBAP Risk Committee.

6.2 Annual review of terms of reference and Committee effectiveness

6.2.1 The Committee shall review annually its terms of reference and its own effectiveness, and recommend to the Board any necessary changes.

6.2.2 The Committee shall report to the Board and inform the Chairman of HBAP Risk Committee how the Committee has discharged its responsibilities and will make recommendations on any action(s) needed to resolve concerns or make improvements.

6.3 Material deviations from core terms of reference

6.3.1 Material deviations from the Group Core Terms of Reference require the endorsement from HBAP Risk Committee.

6.3.2 Notwithstanding the paragraph above, any deviation from the Group Core Terms of Reference that is a consequence of statutory or regulatory requirements taking precedence over the Group Core Terms of Reference, needs to be notified to the Board of the Bank and HBAP Risk Committee.

6.4 Responsibility of subsidiary Risk Committees

6.4.1 The Committee shall :

- (a) review the composition, powers, duties and responsibilities of any Risk Committee of the Bank's subsidiaries;
- (b) oversee the implementation of mechanisms to facilitate the communication and escalation from such subsidiary company committees of matters for the Committee's attention including seeking documentation, certifications or assurances such as copies of minutes, periodic certifications, confirmation of adopting best practice, and other forms of sharing information;
- (c) foster interconnectivity and common governance principles; and
- (d) discuss such matters as the Committee deems appropriate with the chair or other members of such subsidiary committees.

6.5 Reporting to the Board

6.5.1 The Committee will report to the Board on the matters set out in these terms of reference and will provide the Board such additional assurance as it may reasonably require regarding the effectiveness of the Bank's risk management functions.

6.6 External advisers

- 6.6.1 The Committee may retain special counsel, advisers, experts, or other consultants to consider from time to time any matters which the Committee believes are required of it in keeping its responsibilities. The Committee may obtain such professional external advice as it shall deem appropriate to take account of relevant experience outside the Bank and challenge its analysis and assessment. Any such appointment shall be made through the Secretary to the Committee, who shall be responsible, on behalf of the Committee, for the contractual arrangements and payment of fees by the Bank.

6.7 Overlapping responsibilities

- 6.7.1 Where there is a perceived overlap of responsibilities between the Risk Committee and another committee of the Board, the respective committee chairmen shall have the discretion to agree the most appropriate committee to fulfil any obligation. An obligation under the terms of reference of any committee will be deemed by the Board to have been fulfilled, provided it is dealt with by any other committee.

July 2019