HSBC BANK BERMUDA LIMITED AUDIT AND RISK COMMITTEE
CORE TERMS OF REFERENCE

Last reviewed by the Board on 2 November 2023
Last amended on 4 November 2021

1. Purpose

The Board of HSBC Bank Bermuda Limited (the 'Company') has delegated to the Audit and Risk Committee (the 'Committee') oversight of:

1.1 matters relating to financial reporting and internal financial controls, in particular reviewing: (i) the integrity of the financial statements, formal announcements and disclosures relating to financial performance; (ii) the effectiveness of Internal Audit and the external audit process; and (iii) the effectiveness of internal financial control systems; and

1.2 risk-related matters impacting the Company and its subsidiaries, including risk governance and internal control systems (other than internal controls over financial reporting).

2. Membership

The Committee (including the Chair) shall comprise at least three members, all of whom shall be non-executive directors, or as otherwise required by local regulation.

The Chair of the Committee shall be appointed by the Board from among the non-executive directors.

Members of the Committee of any Group subsidiary other than a Principal Subsidiary shall be appointed subject to endorsement by the nomination committee (or equivalent) or audit/risk committee of the entity with oversight responsibility of the Company

At least one member of the Committee shall have recent and relevant financial experience. When appointing directors to the Committee, the Board shall have regard to the Committee collectively to have appropriate skills, experience and competence in relation to financial management relevant to the financial services sector.

3. Attendance

The Committee may invite any director, executive, independent auditor or other person to attend any meeting(s) of the Committee as it may from time to time consider desirable to assist the Committee in the satisfaction of its responsibilities.

The Committee shall meet separately with the external auditor, the Regional Head of Internal Audit, or equivalent, and with the Chief Risk Officer ('CRO') at least twice each year without management present.

4. Meetings and Quorum

The Committee shall meet with such frequency and at such times as it may determine, subject to regulatory requirements.

The quorum for meetings is a majority of the members, including the Chair (or his/her delegate from among the members).

The Secretary of the Committee is the Company Secretary (or his/her nominee).

5. Audit-related Committee Responsibilities

The Committee's responsibilities shall include:

5.1 Financial Reporting

5.1.1 monitor and critically assess the integrity of the financial statements of the Company, and any formal announcements and supplementary regulatory information relating to the Company's financial performance;

5.1.2 review, and consider changes to, significant accounting policies and disclosure practices, as applicable;

5.1.3 review, and report to the Board on, significant accounting judgements and adjustments;

5.1.4 review going concern assumptions and any qualifications;

5.1.5 review, as applicable, compliance with accounting standards, listing rules, and other requirements relating to financial reporting;

5.1.6 review disclosure that describes the work of the Committee;

5.1.7 review the Annual Operating Plan and Capital Plan;

5.1.8 review comment letters from regulatory authorities;

5.1.9 review matters as advised by Internal Audit, any other function or the external auditor;

5.1.10 review any significant or unusual items that may need to be highlighted in the annual report and accounts, or its local equivalent, by the external auditor;

5.1.11 at its discretion, review reports and minutes of the Disclosure Committee, or

its local equivalent if any;

5.1.12 advise the Board whether the annual report and accounts, or equivalent, taken as a whole, are fair, balanced and understandable, and provides the information necessary for shareholders to assess the Company's position and performance, as applicable in the Company's jurisdiction; and

5.1.13 report and provide assurances to the Board on the Company's compliance with all applicable corporate governance codes or standards in relation to financial reporting.

5.2 Internal Audit

5.2.1 review and, if appropriate, approve the Internal Audit charter;

5.2.2 oversee the work of Internal Audit;

5.2.3 monitor and assess the effectiveness, performance, resourcing, independence and standing of the Internal Audit function;

5.2.4 consider major findings of internal investigations and management's response;

5.2.5 approve the local Internal Audit annual work plan including the time assigned to complete each audit, and any material plan changes during the year;

5.2.6 satisfy itself that the Internal Audit work plan is aligned to the key risks of the business;

5.2.7 satisfy itself there is appropriate co-ordination between Internal Audit and the external auditor; and

5.2.8 to request that management inform other Board committees 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.

5.3 External Audit

5.3.1 review the terms of appointment, re-appointment, or removal of the external auditor and approve their remuneration and terms of engagement, and make recommendations to the Board for approval by the Company's shareholder;

5.3.2 oversee the implementation by management of the HSBC Group policy on

the engagement of the external auditor to supply non-audit services, taking into account relevant regulatory requirements;

5.3.3 approve in advance the supply of any non-audit services by the external auditor: (a) considering the impact this may have on independence, (b) taking into account the relevant regulations and ethical guidance in this regard, (c) agreeing the terms of engagement and (d) the fees for any such services; and report to the Board on any improvement or action required;

5.3.4 review and monitor the external auditor's independence, objectivity and the quality and effectiveness of the audit process, considering relevant professional, regulatory and other requirements;

5.3.5 oversee the rotation of audit partners and external auditors;

5.3.6 review the external auditor's report on the progress of the audit, its management letter, any material queries raised by the external auditor to management (and management's responses).

5.3.7 discuss with the external auditor the approach, nature, and scope of their audit and reporting obligations throughout the audit process including, as applicable:

- any significant accounting and auditing problems and reservations;
- major judgemental areas;
- alternative accounting treatments together with the potential ramifications;
- any significant accounting adjustments;
- the going concern assumption and viability statement;
- compliance with accounting standards, stock exchange rules and legal requirements;
- reclassifications or proposed additional disclosures;
- any material changes in accounting policies and practices, any communications provided by the external auditor to management and other matters the external auditor wishes to discuss; and

5.3.8 oversee the implementation by management of the HSBC Group policy for the engagement of former employees and contractors of the external auditor.

5.4 Internal Controls

5.4.1 review the effectiveness of the Company's and its subsidiaries' internal financial controls (the systems established to identify, assess, manage and monitor financial risks);

5.4.2 consider any findings of major investigations of internal controls over financial reporting matters, management's response and the conclusions of any testing carried out by internal or external auditors;

5.4.3 review all significant deficiencies and material weaknesses in the design or operation of internal controls over financial reporting (including any annual report, and other reports as required by applicable laws and regulations, from the Company's Chief Executive and Chief Financial Officer (or equivalent) that such persons have disclosed to the Committee and to the external auditor) which could adversely affect the Company's ability to record and report financial data and any fraud, whether material or not, that involves management or other employees who have a significant role in the Company's internal financial controls; and

5.4.4 review, and, if appropriate, endorse the content of the statement relating to internal financial controls in the annual report, or its equivalent, for submission to the Board.

5.5 Whistleblowing

5.5.1 oversee the local implementation of the Group's policies and procedures for capturing and responding to whistleblower concerns and oversee the local implementation of the Group's procedures to ensure confidentiality, protection and fair treatment of whistleblowers; and

5.5.2 annually review the operation and effectiveness of the arrangements by which staff may, in confidence, raise concerns.

6. Risk-related Committee Responsibilities

The Committee's responsibilities shall include:

6.1 Risk-related Matters

6.1.1 To oversee and advise the Board on risk-related matters, including both financial (including capital & liquidity, retail and wholesale credit risk, strategic risk, and market risk) and non-financial risks (including resilience risk (incorporating information technology, cyber security and third party risk), financial crime and fraud risk, regulatory compliance risk, people risk, legal risk, model risk, and financial reporting and tax risk).

6.1.2 To review and provide independent challenge on risk management reports, including the Company's enterprise risk reports to:

(a) Assess the risk profile of the Company and how the risks arising from the Company's businesses are controlled, monitored and mitigated;

(b) Focus on current and forward-looking risks to enable the Committee to assess the Company's vulnerability and resiliency to potential risks;

(c) Review the effectiveness of the Company's conduct framework designed to deliver fair outcomes for customers, preserve the orderly and transparent operation of financial markets, and protect the Company against adverse outcomes (including reputational damage) to the

Company'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.

6.2 Risk Appetite

6.2.1 To satisfy itself that risk appetite informs the Company's strategy (including technology strategy and climate 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;

6.2.2 To advise the Board on risk appetite and risk tolerance related matters;

6.2.3 To review and recommend the Company's Risk Appetite Statement at least annually to the Board for approval;

6.2.4 To receive reports where appropriate, to satisfy itself that the Company's approach to the determination of its risk appetite is in line with regulatory requirements;

6.2.5 As applicable, to review and recommend the Company'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 the subsidiary/ entity which has oversight;

6.2.6 As applicable, to review and recommend the Company's Internal 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 the subsidiary/ entity which has oversight;

6.2.7 To consider and advise the Board on the risks associated with proposed strategic acquisitions/disposals, focussing in particular on risk aspects and implications for the risk appetite and tolerance of the Company;

6.2.8 To review and advise the Board or other committee that oversees remuneration matters on the Company's alignment of remuneration with risk appetite;

6.2.9 To consider and advise the Board on the effectiveness of management's policies for addressing risks relating to cyber security and information security;

6.2.10 To review and advise the Board on the effective management of risks relating to the Company's IT and operational resilience, including risks relating to the execution of the technology aspects of the approved Group or Company strategy, cyber security and serious, large scale, organised crime

relating to information security; and

6.2.11 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 anti-money laundering, sanctions, terrorist financing and proliferation financing;
(b) Controls relating to anti-bribery and corruption; and
(c) Where the Company may become exposed to financial crime and systems abuse.

6.3 Stress Testing

6.3.1 To review and satisfy itself that the Company's stress testing framework, governance and related internal controls are robust;

6.3.2 To review and challenge management's interpretation of the scenario(s) prescribed by the regulator, including areas of judgement;

6.3.3 To review and challenge the results of, and supporting information for, enterprise-wide stress tests presented by management; and

6.3.4 To review and approve, or recommend for Board approval, the Company's final stress testing submissions to regulatory authorities.

6.4 Enterprise Risk Management Framework and Internal Control Systems

6.4.1 To annually review the Company's enterprise risk management framework and satisfy itself that it is operating effectively;

6.4.2 To review the effectiveness of internal control systems (other than internal controls over financial reporting); and

6.4.3 To review how effectively management is embedding and maintaining an effective risk management culture and a strong internal control environment designed to foster compliance with HSBC Group and Company policies and regulatory compliance requirements.

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.

6.5 Regulatory Compliance

6.5.1 To review the annual plan for the Regulatory Compliance function and receive regular reports on progress against the plan and other matters relating to regulatory compliance risk and the Company's relationship with its regulators.

6.6 Chief Risk Officer and Risk Management Function

6.6.1 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 stature, independent of the business and adequately resourced; and

6.6.2 To recommend to the Board the appointment or removal of the CRO

6.7 Internal Audit

6.7.1 To review reports from Internal Audit that provide assurance on the adequacy of internal control processes; and

6.7.2 To request that management inform 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.

6.8 External Audit

6.8.1 To review any issue raised by the external auditor in respect of (a) the audit of the Company'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 Company's (i) regulatory standing and compliance or (ii) general competitive standing.

6.9 Annual Report and Accounts (or local equivalent)

6.9.1 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 Company.

7. <u>Other responsibilities</u>

7.1 Reporting, Certificates and Assurances (Escalation)

(a) To provide half-yearly certificates to the audit/risk committee of the entity with oversight responsibility of the Company (in a form that is consistent with that required by the Group Audit/Risk Committee); and

(b) To take action, provide documentation or assurances as requested by the audit/risk committee of the entity with oversight

responsibility of the Company including: copies of minutes, periodic certifications, adopting best practice, being forthcoming in sharing information, and interacting with its Chair on a regular basis.

7.2 Annual Review of Terms of Reference and Committee Effectiveness

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

The Committee shall report to the Board and inform the Chair of the audit/risk committee of the entity with oversight responsibility of the Company, how the Committee has discharged its responsibilities and will make recommendations on any action(s) needed to resolve concerns or make improvements.

7.3 Material Deviations From Core Terms of Reference

Material deviations[1] from the Group Core Terms of Reference require the endorsement from: the Board or relevant committee of the entity with oversight responsibility of the Company (where the Company is not a Principal Subsidiary), as and when a material deviation occurs.

[1] Material deviations shall refer to lessening or diminishing of responsibilities contained in the Group Core Terms of Reference. For the avoidance of doubt: (i) enhancements or additions to the Company's Terms of Reference, including additions required under local rule, regulation or law (including PRA Rulebook: Ring-fenced Bodies clauses) and (ii) removal of optional/ alternate language that is not relevant to the Company (specifically due to the fact that the Company is or is not a Principal Subsidiary; or has/ does not have independent non-executive directors), do not need to be escalated for approval.

7.4 Responsibilities of Subsidiary Audit and Risk Committees

The Committee shall (a) review the composition, powers, duties and responsibilities of any audit/ risk committee of the Company'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.

7.5 Reporting to the Board

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 Company's finance, audit and risk management functions.

7.6 External Advisers

The Committee may retain special counsel, advisers, experts, or other consultants to consider from time to time any other matters which the

Committee believes are required of it in keeping with its responsibilities. The Committee may obtain such professional external advice as it shall deem appropriate to take account of relevant experience outside the Company and challenge its analysis and assessment. Any such appointment shall be made through the Company Secretary, who shall be responsible, on behalf of the Committee, for the contractual arrangements and payment of fees by the Company.

7.7 Overlapping Responsibilities

Where there is a perceived overlap of responsibilities between the Committee and another committee of the Board, the respective committee Chairs 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.