HSBC BANK BERMUDA LIMITED AUDIT AND RISK COMMITTEE
CORE TERMS OF REFERENCE
EFFECTIVE 1 JANUARY 2025

Last reviewed by the Board on 30 October 2025
Last amended on 31 October 2024

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 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 control systems; and

1.2 risk-related matters impacting the Company and its subsidiaries, including risk governance.

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

Only members have the right to attend Committee meetings. 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 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 sufficient notice and 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 their delegate from among the members).

The Secretary of the Committee is the Company Secretary (or their nominee).

5. Audit-related areas of responsibility

The Committee's responsibilities shall include:

5.1 Financial reporting and planning

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 consider the effectiveness of model risk management for financial reporting;

5.1.5 review going concern assumptions and any qualifications and provide confirmation to the Board of the Company's profitability;

5.1.6 review compliance with applicable accounting standards, corporate governance codes or standards and other requirements relating to financial reporting, and report and provide assurances to the Board on the Company's compliance;

5.1.7 review disclosure that describes the work of the Committee and areas of special interest;

5.1.8 review the annual financial resource plan, including annual budget, capital expenditure and business plans;

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 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

5.1.12 review comment letters from audit regulatory authorities relevant to the scope of the Committee's responsibilities and activities;

5.2 Internal Audit

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

5.2.2 oversee the work of Internal Audit;

5.2.3 To review reports from Internal Audit that pertain to the purpose and the areas of responsibility of the Committee, including the Internal Audit annual work plan;

5.2.4 monitor and assess the effectiveness, performance, resourcing, independence and standing of the Company's Internal Audit team;

5.2.5 consider significant findings of internal investigations and management's response;

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

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

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

5.2.9 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, considering relevant professional, regulatory and other requirements;

5.3.5 oversee the rotation of the Company's lead 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 controls with input from the Board as appropriate, including (i) how effectively management is embedding and maintaining a strong internal control environment, and (ii) actions to remediate controls which are identified as not operating effectively;

5.4.2 oversee the outputs from monitoring and assurance activities over the Company's internal controls, including areas for enhancement;

5.4.3 consider any findings of major investigations of internal controls, management's response and the conclusions of any testing carried out by the business line, risk function or internal or external auditors;

5.4.3 review all significant deficiencies and material weaknesses in the design or operation of internal controls, and associated remediation plans. Additionally, review other material control deficiencies in the broader control environment which are identified by management, Internal Audit or the external auditors; and

5.4.4 review, and recommend for approval by the Board all internal control-related disclosures within the annual report and other reports required by applicable laws and regulation. .

5.5 Whistleblowing

5.5.1 oversee and annually review the local operation and effectiveness 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 review reports setting out local cases, the key themes and trends, and actions taken to address these.

6. Risk-related areas of responsibility

The Committee's responsibilities shall include:

6.1 Risk-related Matters

6.1.1 To oversee and advise the Board on risk-related matters, comprising 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), ESG risk (incorporating climate 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) enable the Committee to assess the risk profile of the Company and how the risks arising from the Company's businesses are controlled, monitored and mitigated by management;

(b) provide clear 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) enable the Committee to provide such additional assurance as the Board may require regarding the reliability of risk information submitted to it; and

(e) enable the Committee to assess the Company's framework of controls and procedures designed to identify areas where HSBC may become exposed, and through that exposure the financial system more broadly may be exposed, to financial crime or system abuse.

6.2 Risk Appetite

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

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

6.2.3 To review and, if required, recommend the Company's Risk Appetite Framework, on an annual basis, to the Board for approval;

6.2.4 To review and recommend the Company's Risk Appetite Statement on an annual basis to the Board for approval;

6.2.5 To receive reports and draw independent external advice, where appropriate, to satisfy itself that the Company's approach to the determination of its risk appetite is in line with regulatory requirements;

6.2.6 To review and recommend material regulatory submissions to the Board for approval, including the Internal Capital Adequacy Assessment Process and Internal Liquidity Adequacy Assessment Process, satisfying itself with regards to the completeness of the submissions and their consistency with the principles of the Company's Risk Appetite;

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

6.2.8 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;

6.2.9 To review and advise the Board and/or the Remuneration Committee on alignment of remuneration with risk appetite and conduct;

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, challenge and where appropriate, approve the key assumptions, vulnerabilities and scenario themes identified and expanded metrics to be used in both internal and regulatory Company-wide stress tests and regulatory submissions;

6.3.3 To review and approve, or recommend for Board approval, final Company-wide internal and regulatory Stress Tests, including submissions to the Bermuda Monetary Authority or any other regulatory authority.; and

6.4 Risk Management Framework and Internal Control Systems

6.4.1 To review the Company's risk management framework annually;

6.4.2 To oversee implementation of risk data aggregation and risk reporting principles and review and, if required, approve the Company's risk data aggregation and risk reporting framework ; and

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

In carrying out its oversight role, the Committee will :

6.4.3.1 consider any material findings from regulators relating to risk governance, conduct of business, risk assessment or management processes;

6.4.3.2 review the Company's controls relating to compliance risks and satisfy itself that they are adequate and that the Company is maintaining an appropriate relationship with its regulators;

6.4.3.3 consider risk management reports;

6.4.3.4 receive Internal Audit reports relating to weaknesses in risk management and control systems;

6.4.3.5 report to the Board on the effectiveness of risk management.

6.5 Chief Risk Officer and the Risk Management Function / Chief Compliance Officer and the Compliance Function

6.5.1 To monitor the effectiveness and independence of the Chief Risk Officer ("CRO") and Chief Compliance Officer ("CCO) and to review the composition and effectiveness of the Risk function and Compliance function including that they are of sufficient stature, independent of the business and adequately resourced (qualifications, experience and training of staff).

6.5.2 The Committee shall ensure the CRO & CCO:

6.5.2.1 participate in the risk and compliance management and oversight on an enterprise-wide basis;

6.5.2.2 are satisfied that risk owners in the business lines are aware of, and aligned with, the Company's risk appetite;

6.5.2.3 have direct access to the Chair of the Committee;

6.5.2.4 report to the Committee, alongside the internal reporting line to the Chief Executive; and

6.5.2.5 are independent from individual business units

6.5.3 To recommend to the Board the appointment or removal of the CRO and CCO.

6.6 External auditors

6.6.1 To review and track remediation of any issue raised by the external auditor in respect of the audit of the Company's annual report and accounts (and management's response).

6.7 Annual report and accounts (or local equivalent)

6.7.1 Where applicable, to review and endorse the content of the Risk Committee report in the annual report and accounts. In recommending the Risk Committee report to the Board, the Committee shall focus on the following:

6.7.1.1 the Company's risk disclosures, including the articulation of the Company's strategy within a risk management context, including inherent risks to which the strategy exposes the Company, the associated risk appetite and tolerance and how actual risk appetite is assessed over time;

6.7.1.2 forward looking information indicating the expected impact of

potential risks facing the Company; and

6.7.1.3 the articulation of how the different risk areas are managed across the Company and the role of the Committee in providing oversight.

6.7.2 To review and endorse all risk-related disclosures that are contained in the annual report for submission to the Board.

6.8. Other responsibilities

6.8.1 To consider whether external advice on risk matters should be taken, in particular to challenge analysis undertaken and assessments made by the Committee and the Risk and Compliance function. Where it is deemed necessary, the Committee is authorised by the Board to obtain such professional external advice.

6.8.2 Whilst in force, the Committee will have responsibility to oversee compliance with the requirements of all relevant directions, notices and orders.

7. Operation of the Committee

7.1 Escalations

The Committee shall escalate any matters that may have a material impact on the Company or the Group, to the Chair of the Group Audit/Risk Committee respectively. *Refer to the Subsidiary Accountability Framework for guidance on escalations.*

7.2 Reporting and half-yearly certificates

The Committee:

(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.

7.3 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.

8 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.