HSBC HOLDINGS PLC
GROUP RISK COMMITTEE

Approved by the Board on 20 June 2024

Terms of Reference

1. Purpose

The Board of HSBC Holdings plc (the "Company") has delegated responsibility to the Group Risk Committee (the "Committee") for the oversight of risk related matters and the enterprise risks, impacting the Company and its subsidiaries (the "Group"), and risk governance.

2. Membership

The Committee (including the Chair) will comprise of at least three members, all of whom shall be independent non-executive directors.

The Chair of the Committee shall be appointed by the Board.

3. Attendance

Only members have the right to attend Committee meetings. Any other person can attend, by invitation of the Chair for the whole or part of the meeting.

4. Meetings and quorum

The Chair shall ensure that the Committee meets with sufficient notice and frequency.

The quorum for meetings is two members, including the Chair or their delegate from among the members.

The Secretary of the Committee is the Group Company Secretary and Chief Governance Officer (or their nominee).

5. Responsibility of the Chair

The Chair's role requires:

- Fostering an open, inclusive and, where appropriate, challenging discussion;
- Ensuring the Committee has the information necessary to perform its tasks and devotes sufficient time and attention to the matters within its remit;
- Facilitating the running of the Committee to assist it in providing independent oversight of executive decisions;
- Safeguarding the independence of, and overseeing the performance of, the Risk and Compliance Function; and
- Reporting to the Board on the Committee's activities.

6. 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 risks (including capital and liquidity, retail and wholesale credit risk, strategic risk, and treasury and traded 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 Group's enterprise risk reports, to:

- enable the Committee to assess the risk profile of the Group and how the risks arising from the Group's businesses are controlled, monitored and mitigated by management;
- provide clear focus on current and forward-looking risks to enable the Committee to assess the Group's vulnerability and resiliency to potential risks;
- review the effectiveness of the Group's conduct framework designed to deliver fair outcomes for customers, preserve the orderly and transparent operation of financial markets, and protect the Group against adverse outcomes (including reputational damage) to the Group's financial and non-financial condition and prospects;
- enable the Committee to provide additional assurance as the Board may require regarding the reliability of risk information submitted to it; and

- enable the Committee to assess the Group'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.

6.1.3 To conduct forward looking thematic reviews and deep dives to address key risks and areas of regulatory concerns.

6.2 Risk Appetite

6.2.1 To satisfy itself that risk appetite informs all aspects of the Group'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 recommend the Global Risk Appetite Framework, on an annual basis, to the Board for approval.

6.2.4 To review and recommend the Group Risk Appetite Statement, on an annual basis, to the Board for approval. An interim recalibration of risk appetite will take place, as required.

6.2.5 To receive reports and draw independent external advice, where appropriate, to satisfy itself that the Group'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, the Individual Liquidity Assessment Process, the Group Recovery Plan, Resolvability Assessments and Solvent/Trading Activity Wind Down, satisfying itself with regards to the completeness of the submissions and their consistency with the principles of the Group's Risk Appetite.

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

6.2.8 To review and advise the Board on the effective management of risks relating to the Group's Operational and IT Resilience, including risks relating to the execution of the technology aspects of the approved Group 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.

6.2.10 To approve the Group's cost of equity on an annual basis.

6.3 Stress Testing

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

6.3.2 To review, challenge and approve the key assumptions, vulnerabilities and scenario themes identified and expanded metrics to be used in both internal and regulatory Group-wide stress tests and regulatory submissions for material submissions only.

6.3.3 To review and approve final Group-wide internal and regulatory Stress Tests, including submissions to the Prudential Regulatory Authority, the Bank of England, the European Banking Authority or any other regulatory authority.

6.4 Enterprise risk management framework and internal control systems

6.4.1 To review the Group's risk management framework annually and consider a report from Internal Audit that it is operating effectively across the Group.

6.4.2 To oversee implementation of risk data aggregation and risk reporting principles and review and approve the Group's risk data aggregation and risk reporting framework.

6.4.3 To review how effectively management is embedding and maintaining an effective risk management and control system and culture to foster compliance with HSBC Group policies and 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 Group's controls relating to compliance risks and satisfy itself that they are adequate and that the Group 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; and

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

6.5 Internal Audit

6.5.1 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, which should include an evaluation of the effectiveness of the Risk and Compliance function.

6.5.2 To respond to other Internal Audit matters referred to it by the Group Audit Committee.

6.5.3 To ensure that the Group Audit Committee is advised of the Committee's work in relation to Internal Audit reports and, in particular, any shortcomings perceived in the scope or adequacy of the work of Internal Audit.

6.6 Group Chief Risk and Compliance Officer and Risk Management Function

6.6.1 To monitor the effectiveness and independence of the Group Chief Risk and Compliance Officer ("GCRCO") and to review the composition and effectiveness of the Risk and Compliance function including that it is of sufficient stature, independent of the business and adequately resourced (qualifications, experience and training of staff).

6.6.2 The Committee shall ensure the GCRCO:

6.6.2.1 participates in the risk and compliance management and oversight on an enterprise-wide basis;

6.6.2.2 is satisfied that risk owners in the business lines are aware of, and aligned with, the Group's risk appetite;

6.6.2.3 has direct access to the Chair of the Committee;

6.6.2.4 reports to the Committee, alongside the internal reporting line to the Group Chief Executive; and

6.6.2.5 is independent from individual business units.

6.6.3 To recommend to the Board the appointment or removal of the GCRCO.

6.7 External auditors

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

6.8 Annual report and accounts

6.8.1 To review and endorse the content of the Group Risk Committee Report in the annual report and accounts. In recommending the Group Risk Committee Report to the Board, the Committee shall focus on the following:

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

6.8.1.2 forward looking information indicating the expected impact of potential risks facing the Group; and

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

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

6.9 Risk Committees of the Company's Principal Subsidiaries

The Group's principal subsidiary companies are shown in Appendix 1 attached to these terms of reference. The Committee's responsibilities in relation to these subsidiary companies are as follows:

6.9.1 To review the core terms of reference for adoption by such committees and approve material deviations.

6.9.2 To work and liaise as necessary with the Group's principal subsidiaries and their risk committees (setting clear expectations for the latter). In exercising its responsibilities, the Committee will have the right to request but not direct principal subsidiary risk committees to take action or provide information and documentation from time to time such as it shall determine. This may include the following:

(i) receiving escalations on the emerging risks or issues of a principal subsidiary company;

(ii) receiving appropriate assurance certificates on demand and at least half-yearly, to support the Group's external reporting;

(iii) encouraging information sharing and best practice to be adopted; and

(iv) encouraging interaction with the Committee and between the chairs of principal subsidiary risk committees.

6.10 Other responsibilities

6.10.1 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.

6.10.2 Whilst in force, the Committee will have responsibility to oversee compliance with the requirements of:

1) the FCA Direction Notice dated 7 July 2020.

7. Operation of the Committee

The Committee:

- Shall meet with the Group Head of Internal Audit at least twice annually.
- Shall meet with the external auditor at least twice annually.
- Shall meet with the GCRCO, without management present, at least twice annually.
- Shall review these terms of reference and its own effectiveness annually, as well as the quality of information it receives and recommend any necessary changes.
- Shall report to the Board on the matters set out in these terms of reference, how the Committee has discharged its responsibilities and will make recommendations on action needed to resolve concerns or make improvements.
- Shall give consideration to the laws and regulations of all applicable jurisdictions and regulators.
- Shall work and liaise as necessary with all other Board Committees (including to determine where there is an overlap or any gaps in responsibilities). The Committee's interaction with other relevant Boards and Committees of the Group

will be reflected in the detailed plans and processes for the Committee which are developed on an ongoing basis throughout each calendar year.

APPENDIX 1

Group Risk Committee

Terms of Reference

Principal Subsidiary companies of HSBC Holdings plc:

The Hongkong and Shanghai Banking Corporation

HSBC North America Holdings Inc

HSBC Bank plc

HSBC Latin America Holdings (UK) Limited

HSBC Middle East Holdings BV

HSBC UK Bank plc