

SECURE TRUST BANK PLC (“STB” or “Company”)

RISK COMMITTEE

TERMS OF REFERENCE

adopted by the Board on 6 October 2016¹

References to the:

- “**Committee**” means the Risk Committee of the Board of STB.
- “**Board**” means the Board of Directors of STB.
- “**Group**” means STB and its subsidiaries.

1. Membership

- 1.1 The Board will appoint the Chairman of the Committee (the “**Chairman**”), who must be an independent Non-Executive Director. In the absence of the Chairman, the remaining members present must elect one member to chair the meeting.
- 1.2 Members of the Committee are appointed by the Board on the recommendation of the Nomination Committee and after consultation with the Chairman. The Committee must comprise at least two members.
- 1.3 All members of the Risk Committee must be independent Non-Executive Directors. At least one member of the Committee must be a member of the Audit Committee of the Board. The Chairman of the Board must not be a member of the Risk Committee.
- 1.4 Appointments to the Committee are for a period of up to three years, which may be extended for no more than two additional periods of up to three years.
- 1.5 Members of the Committee must have the appropriate knowledge, skills and expertise to understand and monitor the risk strategy and risk appetite of the Group.

2. Secretary

The Company Secretary (or his or her nominee) ordinarily acts as the secretary of the Committee (the “**Secretary**”) and will ensure that the Committee receives information and papers in a timely manner to enable full and proper consideration of the issues.

3. Quorum

- 3.1 The quorum necessary for the transaction of business is two members of the Committee, one of whom must be the Chairman or their chosen alternative.

¹ As amended on 18 January 2021, 23 November 2022, 7 February 2023 and 25 January 2024

- 3.2 A duly convened and quorate meeting of the Committee can exercise all or any of the authorities, powers and discretions vested in or exercisable by the Committee.

4. Frequency of meetings

- 4.1 The Committee must meet at least four times in each financial year at appropriate intervals in the financial and regulatory reporting cycle and at such other times as required for the Committee to discharge its responsibilities effectively.
- 4.2 Outside the formal meeting programme, the Chairman will maintain a dialogue with key individuals involved in matters relating to the terms of reference of the Committee, including the Chairman of the Board, the Chief Executive Officer, the Chief Financial Officer, the Chief Risk Officer, the Chief Internal Auditor, the Money Laundering Reporting Officer and the Data Protection Officer.

5. Notice of meetings

- 5.1 Meetings of the Committee will be called by the Chairman or by the Secretary at the request of the Chairman at times set for each financial year and at the request of any of the members of the Committee or at the request of any of these people if they consider a meeting to be necessary:

- (A) the Chairman of the Board;
- (B) the Chairman of the Audit Committee;
- (C) the Chief Executive Officer;
- (D) the Chief Financial Officer;
- (E) the Chief Risk Officer; or
- (F) the Chief Internal Auditor.

Unless otherwise agreed by the Chairman, notice of each meeting confirming the venue, date and time, together with an agenda of items to be discussed, must be forwarded to each member of the Committee, and to other attendees as appropriate, no later than seven days before the date of the meeting. The Chairman can reduce this notice period to whatever the Chairman considers appropriate in the circumstances. So far as practicable, supporting papers will be provided with the notice of meeting.

6. Proceedings of the Committee

- 6.1 Only Committee members have the right to attend Committee meetings. However, the Committee may invite any member of the Board or member of staff to attend all or part of any meeting as and when appropriate or necessary.
- 6.2 Meetings may be held virtually if those participating can visibly see, hear and speak to each other.

- 6.3 At least once a year the Committee will meet the Chief Risk Officer without Executive Directors or other management present.
- 6.4 The Committee may meet separately with any of the Executive Directors without any other Executive Directors or management being present.
- 6.5 The Chairman will be available to the Secretary, the Chief Executive Officer, the Chief Financial Officer, the Chief Risk Officer and the Chief Internal Auditor to discuss any matters of concern about internal controls or compliance with the Group's legal and regulatory obligations, in the widest sense, should this be considered necessary by those individuals.
- 6.6 Although normally decisions are reached on a consensus, in the event of a disagreement, decisions on any matter are made by the majority, with the Chairman having a second, casting vote in the event of a tie. A Committee member who remains opposed to a proposal after a vote can ask for their dissent to be noted in the minutes.
- 6.7 A decision in writing and signed by all the members of the Committee will be as effective as a resolution passed at a Committee meeting. Any written decision will be tabled and noted at a meeting of the Committee.

7. Minutes of meetings

- 7.1 The Company Secretary (or their nominee) will minute the proceedings and decisions of all Committee meetings and record the names of those present and in attendance.
- 7.2 The members of the Committee must, at the beginning of each meeting, declare the existence of any conflicts of interest arising and the Secretary will minute them accordingly.
- 7.3 Draft minutes of Committee meetings will, following review by the Chairman, be circulated to all Committee members as soon as practicable after each meeting. Once approved, minutes must be circulated to all other members of the Board, unless it would be inappropriate to do so in the opinion of the Chairman.
- 7.4 Final signed copies of the minutes of the meetings of the Committee must be maintained as part of the records of the Company.

8. Engagement with Shareholders

- 8.1 The Chairman will attend the Annual General Meeting of the Company to respond to any shareholder questions on the Committee's activities and responsibilities and the report of those activities included in the Annual Report and Accounts. In addition, the Chairman should seek engagement with shareholders on significant matters related to the Committee's area of responsibility.

9. Authority

- 9.1 The Committee can undertake or investigate any activity within its terms of reference. The Committee is entitled to sufficient resources from the Group to undertake its duties and may at any time ask the

Chief Risk Officer and Chief Internal Auditor to carry out such independent reviews as it deems necessary and report back to the Committee. The Authority of the Committee extends across the Group.

9.2 In particular, the Committee can:

- obtain any information and explanations it requires from any employee of the Group or from persons outside the Group to perform its duties;
- obtain, at the Company's reasonable expense, independent legal, accounting or other professional advice on anything which it believes it necessary or desirable to do so;
- publish in the Company's Annual Report and Accounts details of any issues that cannot be resolved between the Committee and the Board; and
- liaise regularly with other committees (and, in particular, the Audit Committee and the Remuneration Committee) considering the impact of risk management and internal controls being delegated to different committees and where there is perceived to be an overlap of responsibilities between the Committee and any other committee, the respective committee Chairmen can agree the most appropriate committee to discharge any responsibility. A delegated responsibility from the Board under the Committee's terms of reference will be deemed fulfilled if it is dealt with by either the Committee or another STB committee.

10. Responsibilities

The Committee exercises its internal control and risk management role through the reports it receives from the Assets & Liabilities Committee, the Executive Risk Committee, the Chief Risk Officer, the Chief Internal Auditor, the Chief Executive Officer, the Chief Financial Officer and other executive management, its engagement with executive management and from internal and external auditors and consultants.

The Committee will:

General

(A) review the likelihood and impact of principal risks materialising, the frameworks to manage principal risks and risk related strategies and the procedures for monitoring the adequacy and effectiveness of this process and mitigating actions taken by management;

(B) consider the Group's risk appetite relative to the current and future strategy of the Group, including advising the Board on the risk aspects of proposed changes to strategy and strategic transactions (such as acquisitions or disposals), ensuring that a due diligence appraisal of propositions is undertaken, focusing in particular on implications for the risk appetite, tolerance and strategy of the Company, and taking independent external advice where appropriate;

(C) oversee the Group's Internal Capital Adequacy Assessment Process and Internal Liquidity Adequacy Assessment Process and outputs from them;

(D) oversee the current risk exposures of the Group and that a sufficient level of risk mitigation is in place;

Risk Profile

(E) review, monitor and understand the risk profile of the Group (through the on-going process of the identification, evaluation and management of all material risks);

(F) review the performance of the Group relative to risk appetite;

(G) review reports relating to any significant risk issues that require, or are subject to, remedial action or recommendation;

Risk Appetite, Frameworks and Limits

(H) recommend for approval by the Board, the frameworks to manage risk appetite and tolerance and advise the Board on risk appetite, tolerance and strategy and the principal and emerging risks, including those related to climate change, that the Company is willing to take in order to achieve its long-term strategic objectives, and approve and monitor the metrics giving effect to the risk appetite frameworks which are used to monitor risk management performance;

(I) subject to any applicable regulatory prudential limits and any directions from the Board, approve liquidity and interest rate risk, trading and lending positions that would be outside limits previously agreed by the Board or the Committee;

(J) recommend to the Board annually risk appetite and related authorities, limits and mandates;

(K) oversee rigorous stress and scenario testing of the Group that addresses the impact of crystallisation of identified risks and threats;

Risk Management Operating Model

(L) confirm that the Compliance function has the necessary authority, resources, expertise and access to all relevant information to enable it to perform its function effectively and that the Risk Management function has adequate independence from the performance of the services they monitor, and give any instructions the Committee considers necessary to enable such matters;

(M) recommend to the Board the appointment and/or removal of the Chief Risk Officer and ensure that the Chief Risk Officer has an unfettered right of access to the Board and to the Committee;

(N) monitor the training and development requirements of the Group designed to ensure the requisite skills are in place to control risk and promote a supportive risk culture;

(O) oversee the day-to-day risk management and oversight arrangements of management;

Operational Risk

(P) oversee all appropriate Operational Risk assessments;

(Q) oversee the Group's business continuity and disaster recovery plans and review the Group's resilience in dealing with information security;

Regulatory and Compliance

(R) monitor the effectiveness of Compliance, and in particular:

- review, at least annually, the Group's risk management frameworks;
- monitor relations with regulators and arrangements for ensuring that the Group complies with legal and regulatory obligations and responsibilities including those related to climate change;
- receive from Compliance and Legal briefings on changes to legal and regulatory requirements;
- approve the planned risk based programme of work including the Group's Compliance and Financial Crime Monitoring Plans;

Conduct Risk

(S) review reports on conduct risk and exercise oversight of and challenge the way management deals with conduct risk;

Credit Risk

(T) review and monitor the credit risk profile of the Group (and any material developments), including reviewing reports on lending outside credit policies (exceptions reporting);

(U) review and recommend to the Board changes to the risk profile of the Group outside the Board approved risk appetite;

Risk Policies

(V) approve the framework for the structure and prioritisation of risk policies for the Group and their tiering according to materiality of risk, and the relevant approval schedule for those policies;

(W) review and approve Group risk policies as set out in the Policy Framework which are for Committee approval;

Financial Risk

(X) review reports on financial regulatory reporting and related matters, including but not limited to the ICAAP, ILAAP, OLAR, Resolution Pack and Recovery Plan;

Other

(Y) review the Group's policies for preventing and detecting fraud across or for the intended benefit of the Group and report any actual, suspected or alleged fraud (involving misconduct or unethical behavior relating to financial reporting) or misrepresentation of assets to the Audit Committee;

(Z) receive and review reports on any breaches of regulatory requirements and exercise oversight of any remedial action relating to any such breaches;

(AA) review regular reports from the Money Laundering Reporting Officer and the adequacy and effectiveness of the Company's anti-money laundering systems and controls;

(BB) advise the Remuneration Committee on risk weightings to be applied to performance objectives incorporated in the incentive structure for Material Risk Takers, and examine whether incentives provided by the remuneration arrangements take into consideration the Group's purpose, culture, values, risk management, capital, liquidity and the likelihood and timing of earnings;

(CC) consider any relevant advice from the Audit Committee or Internal Audit concerning the effectiveness of the current control framework; and

(DD) review regular reports from the Data Protection Officer and review the adequacy and effectiveness of the Group's data protection systems and controls.

11. Reporting responsibilities

The Chairman will report to the Board after each meeting of the Committee on all matters within its duties and responsibilities and must also formally report to the Board on how it has discharged its responsibilities and report on any other issues on which the Board has requested the Committee's opinion.

The Committee will make whatever recommendations to the Board it deems appropriate on any area within its remit where action or improvement is needed. Any such recommendation of the Committee will take effect only if approved by the Board.

The Committee will assist the Board to draw on the results of the ongoing risk monitoring process to obtain sound, appropriately documented evidence to support the relevant statements and confirmations required from the Board in the Company's Annual Report and Accounts, including:

- that the Board has carried out a robust assessment of emerging and principal risks facing the Group, including reviewing the Company's procedures for managing or mitigating principal risks and identifying emerging risks, particularly those that would threaten its business model, future performance, solvency or liquidity;
- how the Board has assessed the prospects of the Company, over what period it has done so and why it considers that period to be appropriate; and
- whether the Board has a reasonable expectation that the Company will be able to continue in operation and meet its liabilities as they fall due over the period of its assessment.

The Committee will approve an annual report on its activities to be included in the Annual Report and Accounts. The Committee must approve the statements to be included in the Annual Report and Accounts concerning: (i) emerging and principal risks facing the Group and how they are being managed; (ii) the Group's risk management framework, including its effectiveness, and strategy; (iii) the assessment of the Group's prospects; and (iv) internal controls including their effectiveness. The

report should include details of the membership of the Committee, number of meetings held and attendance over the course of the year.

The Committee must approve any risk disclosures in the financial statements (including the Company's annual and half-yearly reports, preliminary results announcements, and any other public announcements relating to the financial performance of the Company), in particular the disclosures in the Directors' Report relating to risk management objectives and policies and statements on internal controls and risk management.

12. Other matters

The Committee will:

- be provided with appropriate and timely training, both in the form of an induction programme for new members and on an ongoing basis for all members;
- give due consideration to laws and regulations, the Prudential Regulation Authority Rulebook and the Financial Conduct Authority's Handbook, the UK Corporate Governance Code and the requirements of the Financial Conduct Authority's Listing Rules and the Disclosure Guidance and Transparency Rules sourcebook and any other applicable rules and guidance, as appropriate;
- consider such other matters as may be decided by the Board; and
- arrange for periodic reviews of its own performance and, at least annually, review its constitution and terms of reference to check it is operating effectively and recommend any changes it considers necessary to the Board for approval.