Board Risk Committee: Terms of Reference

1. The Role of the Board Risk Committee

a) The Committee is a committee of the Board of Scottish Building Society from which it derives its authority and was established to assist the Board in fulfilling its oversight responsibilities for risk management across the Society.

2. Membership

a) The Committee is appointed by the Board. All members of the Committee are independent non-executive directors of the Society. The Committee consists of not less than three members and a quorum is two members present in person or by video or audio conference. The Chairperson of the Board may be a member of, but may not chair the Committee.

b) Only members of the Committee have the right to attend Committee meetings. Other individuals such as other members of the Executive or Management team may be invited to attend as and when appropriate and necessary.

c) The Committee may sub-delegate any or all of its powers and authorities as it thinks fit to one or more of its members or the Society Secretary, including, without limitation, the establishment of sub-committees which are to report back to the Committee.

3. Secretary

a) The Society Secretary or his or her nominee shall act as the Secretary of the Board Risk Committee.

4. Meeting Governance

a) The Committee shall meet for the despatch of business as often as it shall find necessary, with expectations of a minimum of 6 full and formal Committee meetings. Additional meetings of the Committee may be held as and when required.

b) The Secretary of the Committee shall call meetings in accordance with the schedule agreed. Additional meetings may be called by any Committee member or at the request of the Chief Executive, Finance Director or the Chief Risk Officer.

c) Unless otherwise agreed, notice of each meeting confirming the venue, time and date together with an agenda of items to be discussed, shall be forwarded to each member of the Committee and any other person required to attend, no later than five working days before the date of the meeting. Supporting papers shall be published on the Board portal for Committee members and emailed to other attendees as appropriate, at the same time.

d) Meetings of the Committee may be conducted when the members are physically present together or by using the form of video and/or audio conferences. Meetings are recorded via Microsoft Teams and are automatically deleted after a two month period.

e) At each meeting, the Committee shall review and evaluate any potential or actual conflict of interest of the Committee members.

f) Questions arising at a meeting shall be resolved by a majority of votes and, in the case of equal votes, the Chairperson of the meeting shall have a second or casting vote.

g) At least once a year, the Committee should meet without the presence of Executive Directors.

h) Written resolutions are permitted but must be undertaken in accordance with the requirements set out in the Society's Rules with written consent required from all Committee members for approval.

5. Minutes of meetings

a) The Secretary shall minute the proceedings of all meetings of the Committee, including recording the names of those present and in attendance.

b) Draft minutes of the Committee meetings shall be circulated promptly to the Chairperson of the Committee. Once approved, minutes should be circulated to all other members of the Committee unless it would be inappropriate to do so.

c) Final signed copies of the minutes of the meetings of the Committee should be maintained for the Society's records.

6. Responsibilities

Risk Control Framework and Risk Management (incl Compliance)

a) Oversee the development, implementation and maintenance of the Society's Risk Management Framework and Risk and Compliance Strategy.

b) Ensure that the Society's Risk function has sufficient resources to fulfil its responsibilities as part of the overall Risk Management Framework.

c) Provide oversight of and challenge to the day-to-day risk management and oversight arrangements of executive management.

d) Provide advice, oversight and challenge where necessary to maintain a supportive risk management culture throughout the Society.

Risk Appetite

e) Consider, at least annually, and recommend for Board approval the Board Risk Appetite Statement and supporting metrics, in the context of the Corporate Plan and stress testing outputs.

f) Ensure that the Corporate Plan is within the overall risk appetite as stated in the Board Risk Appetite Statement.

Policies and Prudential Documentation

g) Review, and recommend to the Board as appropriate, the Board policies of the Society from a risk perspective, on the basis of reports from the Risk Function. The Board Policies are reviewed in accordance with a set timetable, on a rolling basis.

h) Review, and recommend to the Board as appropriate, the Society's key prudential documentation, namely: the Internal Capital Adequacy Assessment Process

(ICAAP); Internal Liquidity Adequacy Assessment Process (ILAAP); Recovery Plan and Resolution Information Pack.

Risk Monitoring and Assurance

i) Review the Society's risk exposures in respect of performance against risk appetite, risk trends and concentrations.

j) Monitor and scrutinise the Society's top risks and the controls in place to mitigate these.

k) Monitor the risks facing the Society, both current and potential, together with an assessment of each risk on a 'gross' and a 'net' basis.

l) Provide oversight to the activities of the following 'first line' committees: ALCO, Retail Credit Committee and Operational Risk Committee.

m) Review independent 'second line' reports, including those from the Chief Risk Officer including appropriate management information and assurance.

n) Review management reports from the Risk function regarding risk aspects associated with major initiatives, such as change projects.

o) Review management reports from the Risk function regarding risk aspects of the Society's pricing model/s.

p) Oversee and provide challenge to the design and execution of mortgage portfolio stress testing, liquidity stress testing and reverse stress testing assumptions.

q) Oversee and provide challenge to the risks impacting the Society's operational resilience, including IT and cyber threats.

r) Oversee the key risk indicators that are not allocated a 'Green' RAG status at each of the 'first line' risk committees.

s) Review and recommend the annual MLRO report to be submitted to the board for noting.

t) Review the Consumer Duty Management Information dashboard presented by management and ensure that the Society is evidencing the delivery of good outcomes for customer consistent with the duty requirements.

Operational and Management Oversight

u) Oversee the Society's corporate insurance cover to ensure that it provides adequate financial protection against the risks associated with the Society's business.

v) Oversee the Society's operations specifically to ensure the fair treatment of customers including vulnerable customers.

w) Oversee the Society's approach to managing climate change from a risk perspective, ensuring that the appropriate management information is being maintained to track the Society's actions and impact.

Compliance

x) To approve the annual Risk Monitoring Plan from a Compliance perspective and to monitor progress against plan.

y) To review and monitor the Compliance function, including considering reports to the Committee on routine Compliance monitoring or on specific items.

z) To ensure that the Society's Compliance function has sufficient resources and the required expertise to fulfil its responsibilities.

aa) To instruct the Compliance function to carry out specific reviews of any area of operations causing concern to the Committee.

bb) To review at least annually compliance with the Bribery Act, the Proceeds of Crime Act, Money Laundering Regulations and other relevant statutes.

Whistleblowing

cc) To review and maintain ongoing oversight of specific issues relating to the Society's arrangements for its employees and contractors to raise concerns in confidence, including whistleblowing, where delegated by the Board.

dd) To review at least annually the Society's Whistleblowing Policy and procedure to ensure it remains up to date, appropriate and accessible to all employees.

7. Delegated Authority from Board

a) The Board has a formal schedule of matters that are reserved to it, and it has delegated authority to the Board Risk Committee, as detailed in the appendix to the Board Terms of Reference.

b) In managing the authorities delegated to the Board Risk Committee, the Board shall receive from the Committee Chair a report on proceedings after each meeting on key decisions and discussions within its duties and responsibilities.

c) The Committee Chair should perform a periodic assessment of whether responsibilities included in the Terms of Reference document have been achieved. The results of this exercise should be reported to the Board and appropriate action should be taken where it is identified that responsibilities have not been realised.

d) The Committee is authorised to make whatever recommendations deemed appropriate on any area within its remit where action or improvement is needed.

8. Other Matters

a) Committee members are authorised to seek any information required from any employee of the Society in order to perform their duties.

b) The Committee is authorised to obtain, at the Society's expense, external legal or other professional advice on any matter within its authority.

c) Non-material changes to these Terms of Reference can be approved by the Chairperson and noted at the next meeting of the Committee.

d) The Committee shall assist the Senior Management Function holder in the escalation of their Prescribed Responsibilities for the Committee in relation to:

- Prescribed Responsibility d: Overall responsibility for the firms policies and procedures for countering the risk that the firm might be used to further financial crime (FCA)

- Prescribed Responsibility k: Responsibility for (a) safeguarding the independence of, and (b) overseeing the performance of, the compliance function in accordance with SYSC 6.1 (Compliance).

- Prescribed Responsibility l: Responsibility for (a) safeguarding the independence of, and (b) oversight of the performance of; the risk function in accordance with SYSC 7.1.21R and 7.1.22R (Risk control).

Date of approval
May 2024