EARL SHILTON BUILDING SOCIETY

Risk and Compliance Committee – Terms of Reference

Constitution

The Board has established a Committee to be known as the Risk & Compliance Committee.

Membership

The Committee comprises three Non-Executive Directors as determined by the Board from time to time. The Committee is required to be competent and relevant to the Society's sector of operations. The Chair of the Committee is appointed by the Board. A quorum shall be two members.

Attendance at meetings

The Committee will meet quarterly. The Chief Executive, the Finance Director, the Risk and Compliance Manager and IS & Estates Manager will normally be in attendance but may be asked to leave the meeting at certain junctures if this is considered appropriate for the consideration of the business of the meeting at that point. Any other director may attend with the consent of the Chair of the Committee, with the Chair of the Audit Committee likely to attend from time to time, and the attendance of any member of staff may be required.

Authority

The Committee may hold additional meetings as it feels appropriate. It may seek any information it requires from its employees and may, at its election, obtain legal or other professional advice and secure the attendance of third party advisors with relevant experience and expertise where it considers this is required to facilitate the business of the Committee.

Duties

- **Risk**

- On a quarterly basis review and challenge the strategic risks of the Society, ensuring they fall within the set risk appetite and the risk mitigations are in place and effective, prior to its submission to the Board.
- On an annual basis primarily review for information the risks held at "other" level (being all non-strategic risks).
- On a quarterly basis review by exception any risk that is outside of risk appetite and / or has materially moved since the last meeting and identify reasons behind this and any mitigating actions that need to be put in place.
- On a quarterly basis review the "All other level" risk, with focus on those risks rated as "very high" or "high".
- On a quarterly basis review any risk which has exceeded its agreed review date schedule.
- Review an annual report on all the risks recorded in the risk register and how these are being managed and mitigated.
- Review on an annual basis the Risk Management Framework to ensure these reflect the current position and provide assurance that the risks facing the Society are being managed.
- On a quarterly basis to review emerging (horizon) risks and risk incidents.
- On a quarterly basis carry out a "deep dive" into two or three of the risk registers in the presence of the risk owner.

- To consider the adequacy of the resources available including capital resources as per the Internal Capital Adequacy Assessment Process (ICAAP). The risk register and the ICAAP, including risk quantum, provide the basis for the Society's risk management framework.
- To consider the Society's Statement of Risk Appetite before its inclusion in the ICAAP document and to review the ICAAP in its entirety.
- To consider the Society's procedures for the prevention and detection of fraud, recommending any necessary changes to the Board.
- To review any instances of fraud or attempted fraud affecting the Society (or a member of the Society, about their savings or deposits or a mortgage account) which might produce (or potentially produce) financial loss or loss of reputation and to consider the appropriate action to be take, recommending to the Board any changes in policies, procedures or controls which are considered necessary to prevent further occurrence.
- To review the Society's Whistleblowing Policy, the Policy on Compliance with the Savings Account Regulations, IT Policy, Policy on the Prevention of Financial Crime, Equality Policy, Conduct Risk Appetite Statement, Continuance Plan, Wholesale Credit Risk Appetite Statement, Social Media Policy, and its combined Anti-Bribery and Procurement Policy and Policy on Gifts and Entertainment, and approve the same.
- To review the Society's Risk Management Framework Policy, Business Continuity Plan, Business Impact Analysis and Cyber Contingency Plan and recommend any changes to the Board.
- To review the IT MI Dashboard and arrange for the Society to take appropriate action where necessary.
- To receive the Recovery Plan and the Resolution Plan and recommend them to the Board.
- To review third party / outsourcing arrangements via an assessment of Management Information
- To oversee the proper management of financial risks from climate change and ensure that adequate resources are devoted to managing those risks, with monitoring of management information by the Committee, or other committees, as appropriate.
- To review internal audit reports.
- To review arrears and forbearance data for conduct risk issues.

- **Compliance**

- To consider and approve the annual Compliance Plan and the resources available to ensure its effectiveness.
- To receive reports from the Society's Risk and Compliance Manager, including those of any advisory nature, and to make recommendations where appropriate toward actions to be taken.
- To review the Society's policies for compliance with statutory and regulatory requirements, including the Compliance Policy and the Mortgage Compliance Policy, and to recommend any changes to the Board.
- As appropriate, to receive reports from either the Society's Executive or a third party which concern compliance with any statutory or regulatory requirements that affect the Society and to recommend any necessary changes to policies or procedures which might be required.
- To monitor the Society's compliance with its obligations under the Data Protection Act 2018 and under any other statutory or regulatory obligation it has towards the lawful processing and retention of personal data.
- To review the half year Complaints return to be submitted to the FCA.

To review any other compliance related topics requested by the Board

- **General**

The meeting should also:

- Review its own terms of reference annually and recommend any changes to the Board;

- Assess and report to the Board on the control effectiveness of the first and second lines of defence;
- Consider future regulatory and similar developments (horizon scanning) and update the Board, as necessary;
- Report to the Board indicating how its responsibilities have been discharged;
- Promptly circulate accurate minutes of the business of the meeting to all members of the Board;
- To review and approve the Vulnerable Customer Policy and oversee the fair treatment of vulnerable customers and to treating all customers fairly.
- To review and approve the Equality, Diversity & Inclusion Policy
- To consider any other relevant matter not specifically referred to above.

Review

These Terms of Reference, and the Committee's effectiveness, are subject to annual review by the Committee, with the Board ultimately approving the Committee's Terms of Reference.

July 2023