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 Chairman 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 Regulation and Compliance Manager, Risk Officer, Financial Controller 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 Chairman of the Committee 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**

- To continually review and monitor procedures for identifying and managing risk, including formal review of the Risk Universe Document and the Risk Register prior to its submission to the Board, and consideration of the adequacy of resources, including capital resources required as per the Internal Capital Adequacy Assessment Process (ICAAP).
- 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, qua 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, Risk Management Framework Policy, Equality Policy, Wholesale Credit Risk Appetite Statement, Social Media Policy, and its Anti-Bribery and Procurement Policy and Policy on Gifts and Entertainment, recommending the same to the Board for approval.

- To review the Society's Business Continuity Plan, Business Impact Analysis and Cyber Contingency Plan and recommend any changes to the Board.
- To review the Society's Continuance Plan and recommend any required changes to the Board.
- To review the Society's Conduct Risk Appetite Statement and recommend any required changes to the Board.
- To review the Society's MIG arrangements having regard to counterparty insurer risk 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.

- **Compliance**

- To consider and approve the annual Compliance Plan and the resources available to ensure its effectiveness.
- To receive reports from the Society's Regulation 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 receive and consider periodic reporting on compliance with the GDPR as given effect in the UK by any statute or statutory instrument that replaces or amends the Data Protection Act 1998.
- 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 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 2018