

Board Risk Committee Terms of Reference

1. Constitution

The Board has established a sub-committee to be known as the Board Risk Committee (“BRC”) to support it in achieving its objectives and responsibilities. The BRC reports directly to the Board.

2. Membership

2.1. The BRC Chair shall be appointed by the Board. The current Committee membership is;

- David Fisher (Chair);
- Gareth Hoskin;
- John Hunt;
- Annette Barnes
- Lynn McManus; and
- Neil Fuller.

2.2. In addition to the members of the Committee, standing invites for attendance are extended to:

- The Chairman;
- The Executive Management Team;
- Any Director having consulted the Committee Chair; and
- The Chief Internal Audit Officer.

2.3. Furthermore, the Committee may require any individual(s) to attend a Meeting, such as other members of the Senior Management Team, Risk, and External Audit.

2.4. The Senior Enterprise Risk Manager is the appointed Secretary to the BRC.

2.5. In the absence of the Committee Chair and / or appointed deputy, the remaining members present shall elect one of themselves to chair the meeting.

3. Quorum

For a quorum to be established, a minimum of three of the above Members must be present.

4. Frequency of Meetings

The BRC will meet at least five times per year. In addition, three “single item” BRC meetings will be held each year to focus on applicable topics. The Chair of the BRC may also convene an additional meeting of the Committee, if in his judgement an issue arises that cannot wait until the next scheduled meeting or any other circumstances where it is deemed appropriate.

5. Notice of Meetings

- 5.1. Meetings of the Committee shall be scheduled annually in advance.
- 5.2. An agenda of items to be discussed and supporting papers shall be forwarded to each member of the Committee and any other person required to attend, no later than 5 working days before the date of the meeting.

6. Minutes of Meetings

- 6.1. The Secretary shall minute the proceedings of all meetings of the Committee, including recording the names of those present and in attendance.
- 6.2. Draft minutes of Committee meetings shall be circulated to the Chair promptly. Once approved, the secretary shall include the minutes in the papers for the next Board Meeting, with a summary of the key items for noting.

7. Duties

The duties of the BRC are categorised as follows:

I. Risk Control Framework and Risk Management:

- a. Oversee the development, implementation and maintenance of the Society's Enterprise Risk Management Framework and annual Risk Strategy.
- b. Consider significant crystallised risk events and direct Management in respect of remedial action and future mitigation.
- c. Provide advice, oversight and challenge where necessary to embed and maintain a supportive risk culture throughout the firm.

II. Risk Appetite:

- a. Receive and approve at least annually the Society's Strategic Risk Appetite (SRA) framework and Primary SRA statements and metrics, in the context of the Corporate Plan and stress testing outputs.
- b. Oversee at least annually changes to the Society's Secondary SRA statements and metrics.

III. Policies and Prudential Documentation/Processes:

- a. Review, approve or recommend to the Board the Society's suite of Level 1 policies as defined within the Enterprise Risk Management Framework (Board approval required for Lending, Market, Liquidity and Funding, Wholesale Credit and the Remuneration policy).
- b. Approve and recommend to the Board the Society's key prudential documentation/processes namely; Individual Capital Adequacy Assessment Process (ICAAP – including Reverse Stress Testing), Individual Liquidity Adequacy Assessment Process (ILAAP), Resolution and Recovery Planning (RP).

IV. Risk Monitoring and Assurance:

- a. Review the Society's risk exposures in respect of performance against risk appetite, risk trends and concentrations.
- b. Monitor the risks facing the Society, current, emerging and potential, together with an assessment of the adequacy of Management actions.
- c. Provide oversight to the activities of the following Executive Committees (with specific focus on delegated principal risks): Assets and Liabilities Committee, Credit Committee, Conduct and Operational Risk Committee, Operational Resilience Committee and Models and Rating System Committee, with issues escalated as appropriate, through relevant MI and Executive Committee Chair summary templates.
- d. Receive and review independent second line reports, including from the CRO, control environment MI and assurance reporting as considered appropriate.
- e. Receive and review first line management reports, which assess the nature and extent of risks facing the Society and consider the adequacy of management actions.
- f. Receive and review Black/Blue sky outlooks/stress testing (Horizon scanning) as part of second line independent reporting;
- g. Receive periodic management reports regarding the risk profile associated with major initiatives, such as change projects and acquisitions.
- h. Receive periodic reports regarding the risk profile associated with climate change.
- i. Receive and review an annual update on the risk acceptance process.
- j. Reviews whether the pricing of liabilities and assets offered to members take fully into account the firm's business model and risk strategy on a portfolio basis.
- k. Review significant risk related FCA & PRA correspondence/actions and monitor progress against these.
- l. The Committee will receive reports on operational events and incidents, in accordance with the requirements of the ERMF. In accordance with the IIA Financial Services Code, the Committee will also receive reports from Internal Audit on incidents that meet the criteria for a 'significant event'.

V. Remuneration:

- a. Challenge and agree the process for Risk adjustment factors in respect of Senior Management rewards with appropriate recommendation(s) made to RemCo.
- b. Annual review of proposed Corporate Objectives and risk management elements of the Remuneration Policy with appropriate recommendation(s) made to RemCo.

8. Authority

The Committee is authorised to:

- Approve the Society's suite of level 1 policies as defined within the Enterprise Risk Management Framework;
- Direct Management in the control, management and mitigation of risk exposures; and
- Approve and direct internal or independent reviews of Society practice or external / peer group activity to inform its considerations.

9. Reporting Responsibilities

- a. The BRC shall, on a regular and timely basis report:
 - To the Board (through its Minutes) summaries of its activities and recommendations.
 - To other Board sub-committees as appropriate.
 - Should any serious matters be identified by the BRC, or its members, they will be reported to the Society Chair and Chief Executive immediately.
- b. Provide a Risk Management Report to be included with the annual Report and Accounts.

10. Other Matters

The BRC shall:

- a) Have access to sufficient resources in order to carry out its duties;
- b) Be provided with appropriate and timely training, both in terms of an induction programme for new members, and on an ongoing basis for all members;
- c) Arrange for a periodic review of its own performance and, at least annually, review its Terms of Reference to ensure that it is operating at maximum effectiveness and recommend any changes it considers necessary to the Board for approval.
- d) Annually reassess the nature, the amount, the format, and the frequency of the information on risk which it is to receive.