

Board Risk Committee

Purpose

- 1) The purpose of the Board Risk Committee ('the Committee') is to monitor the Group's compliance with the Board's approved risk appetite, risk management framework and risk culture.
- 2) The Committee has delegated authority from the Board in respect of the powers and responsibilities set out in these Terms of Reference.

Membership

- 1) The Committee shall consist of not less than three Non-Executive members of the Board, appointed by the Board. The Chairman of the Committee shall be a Non-Executive Director appointed by the Board.

In the absence of the Chairman the remaining members may appoint another Non-Executive Director to chair a particular meeting. However, the Chairman of the Board may not chair a meeting of the Committee.

- 2) The current Committee members are:

T Barratt – Chairman
R Turner
L McKenzie

The Secretary or their nominee shall act as Secretary to the meeting.

- 3) The Chairman of the Committee, in conjunction with the Head of Risk & Compliance, should ensure that new members to the Committee undergo an induction programme and that ongoing training should be available for all members.
- 4) Only members of the Committee have the right to attend Committee meetings. However, the Prudential Risk Manager, Operational Risk Reporting Manager, Financial Crime Specialist and Executives, as well as other members of staff the Committee feels appropriate and necessary may be invited to attend all or part of any meeting. Non-executive directors that are not members of the Committee may attend meetings of the Committee.
- 5) Any conflicts of interest must be declared and recorded in the minutes. The Chairman of the Committee may request that any attendee withdraw from all or part of a meeting.
- 6) The Head of Risk & Compliance is expected to attend all meetings, along with the Chief Compliance Officer. The Head of Risk & Compliance's formal reporting line is to the Chief Executive. However, he also has a reporting line to the Committee through the Chairman of the Committee in respect of matters set out in these Terms of Reference. The removal of the Head of Risk & Compliance requires the approval of the Board.

Quorum

- 1) A quorum shall be two members.

Frequency of Meetings

- 1) The Committee shall meet at least 4 times a year.
- 2) The Secretary may convene a meeting of the Committee at the request of the Chairman of the Committee, a member of the Committee, the Chief Executive or the Chairman of the Board.

Authority

- 1) The Committee is authorised by the Board to:
 - a) Investigate any activity within its terms of reference;
 - b) Seek any information that it requires from any employee of the Group and all employees are directed to co-operate with any request made by the Committee;
 - c) Call any employee to be questioned at a meeting of the Committee;
 - d) Obtain outside legal or independent professional advice at the expense of the Group, such advisers may attend meetings as necessary.

Responsibilities

- 1) Ensure that the Group's Risk Management Structure is adequately resourced and effective across first and second line. Ensure the second line has appropriate access to information to enable it to perform its oversight function.
- 2) Undertake any required induction or training programmes for its members.
- 3) Review and recommend to the Board the Group's Risk Appetite Statements and Limits taking account of the current and future macroeconomic financial and regulatory environment.
- 4) Review and recommend to the Board the Group's Risk Management Framework.
- 5) Review the implementation of the Risk Management Framework ensuring all risks are managed, having adequate resource and a satisfactory control environment.
- 6) Monitor emerging prudential risks, conduct risks and areas of potential concern, in particular those matters identified or highlighted by the regulatory authorities, and satisfy itself that appropriate reviews are undertaken to identify and manage any impact to the Group and its Members in a timely manner.
- 7) Review reports from the Risk Department through quarterly reports from the Head of Risk & Compliance.
- 8) Monitor & review the performance of the Group's Management Risk Committees:
 - (a) Operational Risk and Compliance (ORCC) through quarterly reports from the Head of Risk & Compliance.

- (b) Mortgage Lending Risk Committee (MLRC) through quarterly reports from the Chief Operating Officer.
- (c) Assets and Liability Committee (ALCO) through quarterly reports from the Finance Director.

Including their approval and oversight of policies and reviews delegated by the Board.

- 9) Review and challenge the internal control environment through the review of the output from the annual control self-assessment process.
- 10) Review and recommend to the Board the Risk Appetite Measures to be used to monitor the Group's risk management performance.
- 11) Monitor the Group's current risk exposures, including performance and compliance against high level risk appetite limits and tolerances;
- 12) In conjunction with the Audit Committee, monitor identified risk control failings and weaknesses, and breaches of reporting risk limits, together with the management actions to resolve them.
- 13) Review the Group's material risks and risk events, ensuring appropriate management action is in place to mitigate risks and support a culture of continuous improvement within the Group.
- 14) Oversee and challenge the design and execution of stress and scenario testing.
- 15) Review and recommend to the Board the Group's Internal Capital Adequacy Assessment Process (ICAAP).
- 16) Review and recommend to the Board the Group's Internal Liquidity Adequacy Assessment Process (ILAAP).
- 17) Consider and recommend to the Board for adoption relevant Board policies namely Treasury, Lending, Financial Crime and Recovery & Resolution Plan and to monitor overall compliance therewith.
- 18) Consider and approve the Data Protection Policy and Business Strategy & Change Framework.
- 19) Consider and approve the Stress Testing Policy and Framework.
- 20) Ensure all aspects of the Risk Management Framework are embedded within the ICAAP, ILAAP, Strategic Plan and all other risk policy statements.
- 21) Review material new risks, both internal and external, and consider the requirement and adequacy of due diligence undertaken to appraise such risks.
- 22) Before a decision to proceed is taken, advise the board on any major initiatives such as proposed strategic acquisitions, disposals, change projects or new initiatives, ensuring that a due diligence appraisal of the proposition has been undertaken, focusing in particular on risk aspects and implications for the risk appetite and tolerance of the Group, and taking independent external advice where appropriate and available. New strategic proposals should be accompanied by a second line opinion.

March 2019

- 23) Provide advice, oversight and challenge necessary to embed and maintain a supportive risk culture throughout the Group and a clear three lines of defence operating model.
- 24) Advise the Board on risk strategy, including the oversight of current risk exposures of the Society.
- 25) Oversight and challenge of the day-to-day risk management and oversight arrangements of the executive.
- 26) Undertake oversight as required by the Remuneration Committee on specific risk or conduct elements to the bonus incentive schemes in operation across the Society.

Other matters

The Committee will:

- 1) Have access to sufficient resources in order to carry out its duties;
- 2) Be alert to the possible need for expert advice and support on any risk issue, taking action to ensure that it receives such advice and support as may be necessary to meet its responsibilities effectively. The Committee is authorised to call any employee of the Society for information in order to perform its duties and to obtain, at the Society's expense, outside legal or other professional advice on any matter the Committee reasonably believes it necessary to do so;
- 3) Be provided with appropriate and timely training. The Chairman of the Committee, in conjunction with the Head of Risk & Compliance, should ensure that new members to the Committee undergo an induction programme and that ongoing training should be available for all members;
- 4) Give due consideration to relevant laws, regulations and statements of good practice;
- 5) Oversee any investigation of activities which are within its terms of reference;
- 6) Carry out reviews of its own performance and at least annually, review its constitution and terms of reference to ensure it is operating at maximum effectiveness and recommend any changes it considers necessary to the Board for approval.
- 7) Have the authority to request that any of the Management Risk Committees conduct further investigations and report on any specific matters falling within the Committee's terms of reference.
- 8) Have regard to any advice from the Audit Committee or Internal Audit concerning the effectiveness of the current control framework.
- 9) Be provided with draft Minutes by the Secretary of the meeting.

Reporting

The Chairman of the Committee will:

- 1) Report to the Board on the activities of the Committee at the Board meeting following the meeting of the Committee;

March 2019

- 2) Make recommendations to the Board within the Committee's areas of responsibility;
- 3) Produce a report on the activities of the Committee to be included in the company's annual report; and
- 4) Attend the Annual General Meeting of the Society to respond to any questions relating to the Committee's responsibilities.