

**Principality Building Society
Terms of Reference
Board Risk Committee**

1. Main Purpose:

The role of the Board Risk Committee is to ensure on behalf of the Board that there is a co-ordinated approach towards the oversight and management of key strategic and corporate risks. It should oversee the risk management governance structure in order that the Society's risk profile can be readily understood and risk management resources targeted appropriately. Specifically, the Committee will:

- 1.1 Recommend to the Board the Risk Appetite Statement including risk appetites and tolerances across the full range of risks to which the Society is exposed.
- 1.2 Be satisfied that the Society's business strategy and Medium Term Plan are aligned with the agreed appetite for risk.
- 1.3 Oversee the risk control framework and be satisfied that it remains relevant to the business.
- 1.4 Advise the Board on proposed strategic transactions and that any potential change in the level of risk remains within risk appetite.
- 1.5 Monitor key risk exposures and satisfy itself that appropriate early warning indicators and forward looking indicators are in place and be satisfied that management is exercising appropriate control of risk exposures.
- 1.6 Review, challenge, approve and monitor economic assumptions, stress and scenario tests, including reverse stress scenarios.
- 1.7 Be satisfied that Members and Customers are treated fairly and that fair outcomes are delivered.

2. Membership:

The Committee shall comprise at least three members, all of which shall be independent Non-Executive Directors. The Chair of the Committee shall be appointed by the Board. In the absence of the Committee Chair at a Committee meeting, the remaining members present shall elect one of themselves to chair the meeting. Membership of the Committee will enable the Committee to achieve a holistic approach to risk through cross membership with the Audit, Transformation and Remuneration Committees. The Chair of the Society's Board shall not be a member of the Committee. The Chief Risk Officer shall have direct access to the Chairman of the Board and to the Committee.

The Secretary of the Committee shall be the Society's Secretary or his nominee.

Members shall have appropriate knowledge, skills and expertise to fully understand risk appetite and strategy/members as a whole shall have relevant risk expertise. The committee as a whole shall have competence relevant to the sector in which the company operates.

3. Quorum:

Two Members of the Committee.

4. Attendance:

Only members of the Committee have the right to attend Committee meetings. Other colleagues may be invited to attend all or part of any meeting, as and when appropriate and necessary. In addition to members of the committee, standing invitations for attendance are extended to:

- All members of the Executive Committee
- The Chief Internal Auditor

The Committee may invite the attendance of any other person and may obtain advice from suitable third parties as considered necessary.

5. Frequency of Meetings:

The Committee shall meet no less than four times per annum. Outside of the formal meeting programme, the Committee Chair, and to a lesser extent the other Committee members, will maintain a dialogue with key individuals involved in the Society's risk management governance framework, including the Chair of the Board, Chief Executive Officer, Chief Risk Officer, Chief Financial Officer and Head of Compliance and Conduct Risk.

6. Committee Functions:

Risk Management Framework

- 6.1 To be satisfied that appropriate methods for measuring risk appetite, tolerances and exposures (allied to the Society's Enterprise Risk Management Framework) are in place across the Society.
- 6.2 Oversee the risk management control framework through: ensuring that full coverage of risks is achieved through the risk management committee structure; approval of risk mitigation strategies where appropriate; and supporting the development of an appropriate risk culture.
- 6.3 Approve any changes to the Society's IRB models where those changes are expected to result in a material change. Receive confirmation that the Society's IRB models have been reviewed by the Internal Audit function and that these are attested to be fit for purpose.
- 6.4 To be satisfied that the risk management framework remains suitable having regard to the changing risk and market environments in which the Society operates.
- 6.5 To be satisfied that the risk management framework keeps abreast of regulatory developments.
- 6.6 Be satisfied that the risk of poor conduct and/or poor outcomes for Members and customers is managed and mitigated.

Risk Appetite

- 6.7 To consider at least annually and recommend to the Board for approval the Society's Risk Appetite and risk appetite measures (including limits and tolerances) consistent with the Corporate Plan and stress testing outputs.
- 6.8 To be satisfied that risk appetite measures reflect the Society's strategy, overall objectives and business plans and encompass relevant measures to assess appetite for exposure to the following risk categories:
 - Business
 - Credit
 - Liquidity and Funding
 - Solvency
 - Interest rate
 - Operational
 - Conduct and
 - Legal and Regulatory

Risk Policies and Strategies

- 6.9 Review and approve/recommend to the Board (where appropriate) key policies as set out at Appendix 1.

Architecture

- 6.10 Review, challenge and approve the assessment of capital and liquidity requirements. Having regard to present and future plans assess the adequacy of capital and liquidity resources.

- 6.11 Review, challenge and approve financial and economic assumptions, stress and reverse stress scenarios used within the ICAAP and ILAAP. Recommend the ICAAP and ILAAP to the Board for approval. Understand the circumstances in which the Society would fail and be satisfied that mitigating management actions are feasible.
- 6.12 Assess the adequacy of the Recovery and Resolution Plan (RRP) (including being satisfied that the RRP includes an appropriate suite of Recovery Indicators) making appropriate recommendations to the Board and in particular challenge the feasibility of proposed management actions.

Monitoring

- 6.13 Monitor on-going risk exposure, and assess whether risk exposures fall within agreed risk appetite. Receive reports on the actions being taken to mitigate the principal risks to which the Society is exposed and determine whether resources are being targeted appropriately.
- 6.14 Receive reports and monitor the performance and actions of the Executive Risk Committee (ERC) and the Model Governance Committee (MGC).
- 6.15 Monitor on an on-going basis the Society's actual and forecast capital and liquidity positions.

Other

- 6.16 Consider the impact on the Society's risk profile of any major initiatives and make appropriate recommendations to the Board.
- 6.17 Not less than once per year, the Committee shall review its own performance, 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.
- 6.18 Monitor the independence and objectivity of the Second Line Risk Function and satisfy itself annually that the resources available to that function are adequate.
- 6.19 Recommend to the Board the appointment and/or removal of the Chief Risk Officer.
- 6.20 Review and approve the terms of reference for the ERC and MGC.
- 6.21 Review and recommend to the Remuneration Committee proposals relating to the level participation in variable reward schemes in operation within the Society and provide an opinion to the Remuneration Committee on whether there are sufficient risk management objectives included and where appropriate whether risk weightings attached to these objectives are suitable.
- 6.22 At least annually review and recommend to the Board for approval the Cyber Risk Strategy.
- 6.23 Receive regular reports on the actions being taken to identify and mitigate climate change related risks, the suitability of operational resilience business contingency planning and information security arrangements.
- 6.24 Receive annual reports (or more frequently by way of exception) on the actions being taken to identify and mitigate the risks associated with facilitation of tax evasion and bribery and corruption including an annual report on corporate hospitality offered by the Society.
- 6.25 Determine appropriate training and development for Committee Members both on appointment and on an ongoing basis to ensure that Members of the Committee are appropriately skilled.
- 6.26 Review and approve the statements to be included in the Annual Report concerning the role and responsibilities of the Committee and the action it has taken to discharge those responsibilities.

- 6.27 Work and liaise as necessary with all other board committees ensuring interaction between committees and with the board is reviewed regularly, taking particular account of the impact of risk management and internal controls on the work of other committees.
- 6.28 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. Reporting to the Committee:

- 7.1 The Committee may obtain such information as it considers necessary from any employee or officer of the Society and may obtain legal or other professional advice as it considers necessary. All employees and officers are directed to co-operate with any request made by the Committee.
- 7.2 The Secretary of the Committee shall circulate the Agenda and papers for each meeting of the Committee no less than three working days in advance of the relevant meeting.
- 7.3 Each employee or officer shall ensure that reports for consideration at the Committee are with the Secretary of the Committee no less than five working days in advance of the relevant meeting.

8. Reporting from the Committee:

- 8.1 This Committee reports to the Society's Board.
- 8.2 A summary of the minutes of each meeting of the Committee shall be submitted to the Board.
- 8.3 The Committee shall make whatever recommendations to the board it deems appropriate on any area within its remit where action or improvement is needed.
- 8.4 The Chair of the Committee will provide an oral report on the activities of the Committee to the Board following each meeting of the Committee.
- 8.5 The Committee shall provide advice to the remuneration committee on any risk weightings to be applied to performance objectives incorporated in the incentive structure for executive remuneration and make recommendations to the remuneration committee on clawback provisions.
- 8.6 The Secretary to the Committee will record any conflict of interest disclosed at a Committee meeting.
- 8.7 Delegate any matter or matters to another committee or person(s) as it deems appropriate.

9. Engagement with Stakeholders

- 9.1 The Chair of the Committee shall attend the Annual General Meeting to answer member questions on the Committee's activities.
- 9.2 The Chair of the Committee should seek engagement with stakeholders on significant matters related to the committee's areas of responsibility.

APPENDIX 1

Key Corporate Documents Maintained by the Committee:

- Treasury Policy Statement
- Recovery and Resolution Plan
- ICAAP
- ILAAP
- Lending Policy Statements [Building Society and Principality Commercial]
- Enterprise Risk Management Policy

- Financial Crime Policy
- Cyber Strategy (*forming part of the Information Security Policy*)
- Compliance and Conduct Policy
- Conduct and Compliance Monitoring Plan