

**Approved by the Board of Nationwide Building Society (the Society) on 19 March 2025**

For the purposes of these Terms of Reference, terms shall have the meanings given to them in the Governance Framework document and the “Society Plan” shall mean Nationwide’s Strategy.

**1. PURPOSE**

- 1.1 The purpose of the Board Risk Committee (BRC or the Committee) is to provide oversight and advice to the Board in relation to current and potential future risk exposures and future risk strategy of the Society (on a solo and consolidated basis), including determination of risk appetite and to report formally to the Board on those matters after each meeting. Additionally, the Committee is responsible for monitoring compliance oversight and the effectiveness of the Enterprise Risk Management Framework (ERMF) and advising the Remuneration Committee on any risk adjustments to be made on remuneration.

**2. AUTHORITY**

- 2.1 The Committee is a Committee of the Board and has delegated authority from the Board to which it regularly reports in respect of its functions and responsibilities as set out in these Terms of Reference.
- 2.2 The Committee may sub-delegate any or all of its powers and authority as it sees fit, including, without limitation, the establishment of sub-committees to analyse particular issues and to report back to the Committee.
- 2.3 The Committee has authority to oversee any investigation of activities relating to the Group which are within its Terms of Reference.
- 2.4 The Committee is authorised to seek any information it requires from any employee of the Group in order to perform its duties or call any employee to be questioned at a meeting of the Committee as and when required.
- 2.5 The Committee may obtain, at the Group’s expense, external legal or other professional advice on any matter within its Terms of Reference.
- 2.6 The Committee Chair and the Society Secretary are authorised by the Board to review and approve any non-material change required to be made to the Committee’s Terms of Reference. Any such change should be reported to the Board.

**3. MEMBERSHIP**

- 3.1 Members of the Committee shall be appointed by the Board, on the recommendation of the Nomination and Governance Committee in consultation with the Chair of the Committee.
- 3.2 The Committee shall be made up of at least three independent non-executive directors of the Society, including a member of the Audit Committee and a member of the Remuneration Committee.
- 3.3 The Board shall appoint the Committee Chair who shall be an independent non-executive director.
- 3.4 In the absence of the Committee Chair and/or an appointed deputy, the remaining members present shall elect one of themselves to chair the meeting.
- 3.5 The Chair of the Group shall not be a member of the Committee.
- 3.6 Appointments to the Committee shall be for a period of up to three years, which may be extended for a further three year period (or, in exceptional circumstances, two such periods), provided the director still meets the criteria for membership of the Committee.
- 3.7 Only the members of the Committee have the right to attend Committee meetings. Other individuals such as the Group Chair, Group CEO, Group CRO, other Executive Directors of the Society or VMUK, members of the VMUK board risk committee (VMBRC), external adviser(s), and representatives from relevant business functions of the Group may be invited to attend all or part of any meeting as and when appropriate.

**4. SECRETARY**

- 4.1 The Society Secretary or their nominee shall act as the Secretary of the Committee and will ensure that the Committee receives information and papers in a timely manner to enable full and proper consideration to be given to the issues.

**5. QUORUM AND MODE OF MEETINGS**

- 5.1 The quorum necessary for the transaction of business shall be two members, one of whom must be the Chair of the Committee or their appointed deputy.
- 5.2 A duly convened meeting of the Committee at which a quorum is present shall be competent to exercise all or any of the authorities, powers and discretions vested in or exercisable by the Committee.
- 5.3 In the event of difficulty in forming a quorum, independent non-executive directors of the Society who are not members of the Committee may be co-opted as members for individual meetings.
- 5.4 A decision of the Committee may be taken by written resolution or electronic means. A decision in this instance will be valid only if taken by a quorum as set out in 5.1 above.
- 5.5 The members of the Committee shall be deemed to meet together if they are in separate locations, but are linked by conference telephone, video or other communication equipment. For the avoidance of doubt, a quorum in that event shall be as set out in 5.1 above. Such a meeting shall be deemed to take place where the largest group of members of the Committee participating is assembled or, if there is no such group, where the Chair is located.

**6. FREQUENCY OF MEETINGS**

- 6.1 The Committee shall meet at least four times a year and otherwise as required.
- 6.2 At least once a year, without the presence of executive management, the Committee shall meet with the Group CRO to discuss their remit and any issues arising from the risk oversight activity. In addition, the Group CRO, the Data Protection Officer, the Society's Chief Internal Auditor and the Money Laundering Reporting Officer shall be given the right of direct access to the Committee.

**7. NOTICE OF MEETINGS**

- 7.1 Meetings of the Committee shall be called by the Secretary of the Committee at the request of the Committee Chair.
- 7.2 Meetings of the Committee shall be called by the Secretary of the Committee at the request of any of its members or at the request of external or internal auditors if they consider it necessary.
- 7.3 Unless otherwise agreed, notice of each meeting confirming the venue, time and date together with an agenda of items to be discussed, shall be forwarded to each member of the Committee and any other person required to attend no later than three working days before the date of the meeting.
- 7.4 Supporting papers shall be sent to Committee members and to other attendees as appropriate, at the same time.

**8. MINUTES OF MEETINGS**

- 8.1 The Secretary of the Committee shall minute the proceedings and resolutions of all meetings of the Committee.
- 8.2 The Secretary of the Committee shall record any conflicts of interest reported at the meeting.
- 8.3 Draft minutes of Committee meetings shall be circulated to all members of the Committee and, once agreed, made available to all members of the Board (unless, in the opinion of the Committee Chair, it would be inappropriate to do so).

**9. DUTIES AND RESPONSIBILITIES**

- 9.1 The Committee shall annually, or more frequently as required, establish and recommend to the Board the Society and the Group's Board Risk Appetite metrics, and ensure that the Board considers the appropriateness of the Society's Plan in the context of these Risk Appetites.
- 9.2 The Committee shall approve under delegated mandate from the Board (in relation to the Society and, where applicable, the Group):
  - The ERMF;
  - Recovery Plan
  - Resolvability Self-Assessment
  - Internal Capital Adequacy Assessment Process (ICAAP) and Internal Liquidity Adequacy Assessment (ILAA)
  - Oversight Plan

- 9.3 The Committee shall review and approve on behalf of the Board any Group-wide policies which the Board formally delegates to the Committee.
- 9.4 The Committee shall review the Society's continued assessment of good customer outcomes and actions taken to address any identified risk of actual or potential poor customer outcomes.

## RISK CONTROL FRAMEWORK

The Committee shall:

- 9.5 Keep under review the effectiveness of the ERMF to identify, assess and manage risk within the agreed Society Plan and Board Risk Appetite, ensuring sound systems of risk management and internal control.
- 9.6 Delegate authority to the Group CRO to approve minor revisions to the ERMF in between meetings of the Committee to ensure that they are kept up to date, such revisions being reported to the next appropriate meeting of the Committee. Any significant revisions will be reported to the members of the Committee.
- 9.7 Challenge the Society and the Group's assessment and measurement of key current and longer-term risks.
- 9.8 Challenge the Society and the Group's assessment of compliance with legislative and regulatory requirements.
- 9.9 Provide advice, oversight and challenge necessary to enable management to embed and maintain risk awareness and management in the Society and the Group's culture and to ensure appropriate customer outcomes.
- 9.10 Provide oversight and challenge of the day-to-day risk, control and oversight arrangements of the executive and provide advice to the Board as to the effectiveness of the control environment.
- 9.11 Provide oversight and challenge of the design and execution of scenario analysis, including the review where appropriate of assumptions, results, and proposed management actions on behalf of the Board.
- 9.12 Provide oversight and challenge of due diligence on risk issues relating to material transactions and strategic proposals that are subject to approval by the Board, focussing in particular on implications for the risk appetite, and strategy and taking independent external advice where appropriate.
- 9.13 Provide oversight and challenge so that there is appropriate alignment between the Society and the Group's material products and services (including pricing and profitability) and its values, risk strategy, risk appetite and customer outcomes.
- 9.14 Provide advice on the appointment of external risk consultants that the Group CRO may decide to engage for advice or support.
- 9.15 Keep under review the appropriateness of the Group's Resolvability Self-Assessment up and until any Board Contingency Planning Committee is in operation and make recommendations to the Board for approval.
- 9.16 Review and satisfy itself that the Society and the Group's stress testing framework, governance and related internal controls are appropriate.

## RISK MONITORING

The Committee shall:

- 9.17 Review the Society and the Group's risk profile in respect of performance against risk appetite, risk trends, customer outcomes, emerging risks and risk concentrations.
- 9.18 Receive and review management reports which assess the nature and extent of risks facing the Society and the Group, including reports on any material breaches of risk appetite, and consider the adequacy of proposed actions and the impact on the business of risks that do materialise.
- 9.19 Receive and review management reports on models and scenarios employed in the determination of climate associated risks.
- 9.20 Monitor economic crime related risks including anti-money laundering, anti-bribery and corruption, counter terrorism financing, economic crime, and the financial impact of fraud.
- 9.21 Review regular reports from the Money Laundering Reporting Officer.
- 9.22 Monitor cyber related risks including ransomware recovery, device security, network security, central security control and security of non-production environments.
- 9.23 Monitor the risks associated with outsourcing including disaster recovery and exit plans.

- 9.24 Monitor the deployment of the Society's Recovery Plan, once implemented, and assess the risk of entering into Resolution.
- 9.25 Monitor the performance of the Society's Executive Risk Committee (ERC) within the context of Nationwide's strategy, risk appetite and risk culture, and ERC's Terms of Reference.
- 9.26 To make recommendations to the Board on the appointment and removal of the Group CRO. The Chair of the Committee will be consulted in respect of the Group CRO's performance appraisal and compensation.
- 9.27 The Group CRO's formal reporting line is to the Group CEO. However, the Group CRO also has a reporting line to the Committee through the Chair of the Committee in respect of the matters set out in these Terms of Reference.
- 9.28 The Group CRO will meet regularly with the Chair of the Committee and will have the right and responsibility to elevate issues to the Chair of the Committee where they consider it necessary in the furtherance of their responsibilities.
- 9.29 The Committee shall satisfy itself that the Risk function is adequately resourced, has appropriate access to information and is free from constraint by management or other restrictions so as to be able to perform its function effectively.

#### REMUNERATION

- 9.30 The Committee will provide input to the Remuneration Committee to assist that committee in its assessment of possible impacts on variable remuneration. Such "input" may be provided in conjunction with the Audit Committee including a) an examination of whether remuneration incentives take into consideration capital, liquidity and the likelihood and timing of earnings; b) whether any risk weightings should be applied to performance objectives incorporated in the incentive structure of executive remuneration and c) how incentive & remuneration arrangements appear to have affected observed behaviours & influences on risk culture & any consequent impact on the organisation's principal risks and to make recommendations to the Remuneration Committee on clawback provisions.
- 9.31 The Committee shall review any recommendations, including those made by the Investigations Oversight Committee, to the Remuneration Committee in respect of serious breaches of risk management or significant involvement of Risk and Oversight.
- 9.32 The Committee may refer matters for investigation to the Investigations Oversight Committee as appropriate.

#### OVERSIGHT

- 9.33 The Committee shall monitor and assess the effectiveness of the Second Line Oversight functions in the context of the overall risk management system and review all reports to the Board Risk Committee from the Second Line Oversight functions.

#### ANNUAL REPORT

- 9.34 The Committee shall review and recommend to the Audit Committee for onward recommendation to the Board for its approval the risk statements to be included in the Annual Report concerning internal controls and risk management including a declaration on the effectiveness of the ERMF prior to their endorsement by the Board and the external auditors.

### **10. CONSOLIDATED OVERSIGHT**

#### VM SUB-GROUP

- 10.1 VMBRC is responsible for overseeing the management of risk across the VM Sub-Group, as outlined in its charter.
- 10.2 The BRC is responsible for the risk oversight of the Group and, therefore, exercises oversight over the VM Sub-Group in the context of the Group's consolidated position.
- 10.3 In exercising this oversight, the Committee shall:
  - 10.3.1 review the composition, powers and responsibilities of the VMBRC, including by approving any material changes to its terms of reference; and
  - 10.3.2 work and liaise as necessary with the VMBRC. In exercising its responsibilities, the BRC will have the right to request that the VMBRC take action or provide information, documentation and assistance such as the BRC shall determine.

#### THE MORTGAGE WORKS ("TMW")

- 10.4 The Committee has a responsibility to provide oversight of risk related matters and enterprise risks within TMW and endorse material deviations by TMW from the approach adopted by the Society where they impact the Group.
- 10.5 In exercising its responsibilities, the Committee will have the right to request TMW Directors to take action or provide information and documentation from time to time such as it shall determine.

## 11. REPORTING RESPONSIBILITIES

- 11.1 The Committee Chair shall report formally to the Board on its proceedings after each meeting on all matters within its duties and responsibilities including monitoring the Society and the Group's performance against Board Risk Appetite and approving the ERMF.
- 11.2 The Committee shall make whatever recommendations to the Board it deems appropriate on any area within its remit where action or improvement is needed.
- 11.3 A report to members on the Committee's activities is to be included in the Society's Annual Report and Accounts.

## 12. DECISION MAKING AND SENIOR MANAGER AND CERTIFICATION REGIME RESPONSIBILITIES

- 12.1 All members of the Committee are responsible for and bound by the decisions taken by the Committee whether or not they actively supported or participated in the decisions although dissent can be recorded.
- 12.2 A member of the Committee who is a Senior Management Function (SMF) Holder under the Senior Manager and Certification Regime (SMCR) remains individually accountable for their contributions to collective decisions and their implementation insofar as those contributions are in scope of their Senior Manager responsibilities and therefore they also remain accountable for taking reasonable steps in respect of their function and allocated responsibilities.

## 13. ANNUAL GENERAL MEETING

- 13.1 The Chair of the Committee or a deputy chosen from the Committee membership shall attend the Annual General Meeting to respond to any member questions on the Committee's activities or any matter within the remit of the Committee.

## 14. MISCELLANEOUS

- 14.1 Where there is a perceived overlap of responsibilities between the Committee and the Audit Committee, the respective Committee Chairs shall have discretion to agree the most appropriate Committee to fulfil any obligation. An obligation under the Terms of Reference of the Committee or the Audit Committee will be deemed by the Board to have been fulfilled provided it is dealt with by either of the Committee or the Audit Committee.

The Committee shall:

- 14.2 Give due consideration to applicable laws and including the PRA and FCA's Principles and Rules and associated guidance, the FCA Listing Authority's Listing Rules and Disclosure Guidance and Transparency Rules, the Building Societies Act 1986 and to the recommendations in the UK Corporate Governance Code and FCA's Consumer Duty, as appropriate.
- 14.3 Be cognisant of any conduct risks arising (or increasing) as a result of their judgment and will take proactive steps to avoid or mitigate these risks where possible.
- 14.4 Work and liaise as necessary with all other Board Committees as required.
- 14.5 Have access to sufficient resources in order to carry out its duties, including access to Secretariat for assistance as required.
- 14.6 Receive appropriate and timely training, both in the form of an induction programme for new members and on an on-going basis for all members.
- 14.7 At least once a year, review its own performance, constitution and terms of reference to ensure it is operating effectively and in line with PRA and FCA requirements, and report the results of this review and recommend any changes necessary to the Board for approval.