

Yorkshire Building Society - Group Risk Committee Terms of Reference

Role	The Group Risk Committee (GRC) is a Committee of the Board of Yorkshire Building Society from which it derives its authority. Its role is to oversee Risk Strategy, Appetite and Oversight for the key Prudential, Operational and Conduct Risks, ensuring regulatory compliance and supporting the long-term sustainable success of the Society.
Membership	<p>The Committee will comprise of at least three independent Non-Executive Directors.</p> <p>Members of the Committee will collectively add appropriate knowledge, expertise and professional experience concerning risk management.</p> <p>Appointments to the Committee are made by the Board and will be for a period of up to three years, which may be extended for a maximum of two additional terms provided the Director still meets the criteria for membership of the Committee (and subject to their overall term of office on the Board).</p>
Chair	<p>The Board will appoint the Committee Chair who will be an independent Non-Executive Director.</p> <p>In the absence of the Chair, or an appointed deputy, the remaining members present shall elect one of their number to chair the meeting.</p>
Secretary	The Secretary of the Committee will be the Senior Manager Enterprise Risk Management or their nominee.
Attendees	<p>Only members of the Committee have the right to attend Committee meetings. However, other individuals such as the Chief Executive, Chief Risk Officer, Chief Operating Officer, Chief Financial Officer, Chief Commercial Officer and Chief Internal Audit Officer may be invited to attend for all or part of any meeting, as and when appropriate.</p> <p>In addition, attendance will be open to all Non-Executive Directors who are not members of the Committee, when appropriate.</p>
Frequency	<p>The Committee will normally meet four times a year at appropriate times and otherwise as required.</p> <p>Meetings of the Committee will be called by the Secretary of the Committee or the Group Secretary at the request of its members.</p>
Quorum	<p>The quorum necessary for the transaction of business will be three members.</p> <p>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.</p> <p>In the event of equal votes the Chair of the Committee shall have a casting vote.</p>
Written Resolutions	Written resolutions must be undertaken in accordance with the requirements set out in the Society's Rules with written consent required from all Committee members for approval.
Mandate	<p>The Committee is authorised to:</p> <ol style="list-style-type: none"> 1. Seek any information it requires from any employee of the Society in order to perform its duties. 2. Obtain, at the Society's expense, outside legal or other professional advice on any matter within its terms of reference. 3. Call any employee to attend a meeting of the Committee as and when required. 4. Have the right to publish in the Society's Annual Report details of any issues that cannot be resolved between the Committee and the Board. 5. Approve (ahead of Board approval where relevant) risk strategy and risk appetites for the Society that mandate it to achieve a Board approved Plan whilst protecting outcomes for stakeholders. 6. Oversee all major risks to the Society including (where appropriate) those matters under the Senior Managers & Certification Regime, including safeguarding the independence and overseeing the performance of the Risk and Compliance functions. 7. Provide advice, oversight and challenge necessary to embed and maintain a supportive risk culture throughout the Society.
Responsibilities	<p>The Committee will carry out the duties below for the Society and the Group as a whole and in respect of section 4.1 for Accord Mortgages.</p> <ol style="list-style-type: none"> 1. Duties <ol style="list-style-type: none"> 1.1. Monitoring: <ul style="list-style-type: none"> • CRO Quarterly Report 1.2. Approving: <ul style="list-style-type: none"> • Enterprise Risk Management Framework • Governance, Risk and Control Strategy • Regulatory Risk, Information Management and Information and Cyber Security Policies • Appropriate stress testing including Reverse Stress Tests • ICAAP Pillar 2B scenarios • ILAAP Stress scenarios • Recovery Plan and Resolution Packs (or attestation re ability to produce Resolution Packs during the

- PRA's suspension of the need to produce the Packs)
- Second Line of Defence ('LoD') Oversight Plans (Compliance and Conduct, Prudential, Operational)
- Product approval if product requires change to risk appetite
- Business Control Overlay (Risk) Process for Material Risk Takers' Bonus/SEI
- Due Diligence on strategic transactions (e.g. Mergers/Acquisitions)
- Overall levels of Corporate Insurance, including Directors and Officers Liability
- Delegation of mandates to Sub Committees
- 1.3. Oversight:
 - Second LoD Monitoring (Compliance and Conduct, Prudential, Operational)
 - Management of the financial risks from climate change
 - Operation of the IRB Rating System
 - The requirements of the FCA's Consumer Duty
 - Periodic investigative deep dives into ad hoc areas
- 2. Recommendations to the Board**
- 2.1. Risk Appetite Setting
- 2.2. Risk Policies:
 - Retail and Commercial Lending
 - Funding and Liquidity Risk
 - Capital Risk
 - Treasury Risk
 - Market Risk
 - Financial Crime
 - Procurement, Outsourcing and Third-Party Policy
- 2.3. Regulatory Capital (ICAAP)
- 2.4. Regulatory Liquidity (ILAAP)
- 2.5. Risk Appetite Adherence
- 2.6. Money Laundering Reporting Officer's annual report
- 2.7. Operational Resilience Important Business Services and Impact Tolerances
- 2.8. Operational Resilience Self-Assessment
- 3. Reporting Responsibilities**
- The Committee shall:
 - 3.1. Report formally to the Board through the Committee Chair on its proceedings after each meeting in respect of all relevant matters within its duties.
 - 3.2. Make whatever recommendations to the Board it deems appropriate on any area within its remit where action or improvement is needed.
 - 3.3. Report to the Board on how it has discharged responsibilities which will be included in the Society's Annual Report.
- 4. Senior Managers & Certification Regime Prescribed Responsibilities**
- 4.1. The Committee shall assist the Senior Management Function (SMF) holder in the escalation of their Prescribed Responsibilities for the Committee in relation to:
 - Prescribed Responsibility k - SMF Holder: Chair of Group Risk Committee
Responsibility for a) safeguarding the independence of, and b) oversight of the performance of the risk function in accordance with SYSC 6.1 (Compliance)
 - Prescribed Responsibility l - SMF Holder: Chair of Group Risk Committee
Responsibility for a) safeguarding the independence of, and b) oversight of the performance of the risk function in accordance with SYSC 7.1.21R and SYSC 7.1.22R (Risk Control)
- 5. Other Matters**
- 5.1. Review and maintain ongoing oversight of specific issues relating to the Society's arrangements for its employees and contractors to raise concerns in confidence, including whistleblowing, where delegated by the Board.
- 5.2. The Committee shall give due consideration to laws and regulations, the provisions of the UK Corporate Governance Code and the requirements of the UK Listing Authority's Listing, Prospectus and Disclosure and Transparency Rules and any other applicable Rules, as appropriate. This will include having regard to the various matters set out in Section 172 of the Companies Act 2006 in promoting the success of the Society where relevant.
- 5.3. The Committee shall annually arrange for reviews of its own performance and, at least annually, review its terms of reference to ensure it is operating at maximum effectiveness and recommend any changes it considers necessary to the Board for approval.
- 5.4. The Committee Chair will attend the Annual General Meeting to answer member questions on the Committee's activities.

	5.5. The Committee shall make available its terms of reference explaining clearly its role and the authority delegated to it by the Board.
Sub Committees	<p>Executive Risk Committee (ERC). ERC has delegated authority from Group Risk Committee to ensure the Society's balance between seeking opportunity and managing risk is appropriate:</p> <ul style="list-style-type: none"> • Determining and amending the Society's attitude to risk and setting thresholds for endorsement by Group Risk Committee and Board. • Ensuring that controls are adequately designed and effective to keep the Society within those thresholds. • Monitoring and reviewing the risk exposures of the Society in accordance with the Enterprise Risk Management Framework, Risk Appetite, Group Strategy and the Corporate Plan. • Overseeing that the Society operates compliantly. • Ensuring clear reporting of risk exposures to Group Risk Committee and Board.
Date of Approval	<p>16 October 2023 (GRC recommendation to Board) 13 December 2023 (Board approval)</p>