


**Risk Management**



# Group Risk Committee (GRC)

## Terms of Reference

**Connecting our communities  
with a better financial future**



Approved by GRC 2<sup>nd</sup> October 2024, ratified by Board 29<sup>th</sup> October 2024

# Group Risk Committee (GRC) - Terms of Reference

The Terms of Reference detailed below set out the scope and objectives of the Group Risk Committee (GRC).



## Purpose

The Board has established a Committee of the Board to be known as the Group Risk Committee ("GRC") to oversee the management of risk across the Society. The GRC reports to the Board and is responsible for all material risks, including both conduct and prudential risks. It is also responsible for the Society's risk framework, risk appetite statements and ensuring that these remain consistent with the Society's strategic plan.



## Membership

The GRC shall comprise at least three members, all of whom shall be independent non-executive directors. The GRC shall include at least one member of the audit committee and/or remuneration committee (who may be the same person). Members shall have appropriate knowledge, skills and expertise to fully understand risk appetite and strategy and at least one member shall have recent and relevant financial service experience.

Members of the GRC shall be appointed by the board on the recommendation of the nomination committee and in consultation with the chair of the risk committee. Appointments shall be for a period of up to three years which may be extended for up to two additional three-year periods, provided the director still meets the criteria for membership of the committee.

Only members of the GRC have the right to attend committee meetings. Other regular attendees at meetings of the committee will include the Chief Executive Officer, the Chief Risk Officer, the Chief Internal Auditor, the Chief Financial Officer and other executive directors and other colleagues may be invited to attend all or part of any meeting as and when deemed appropriate. Any other board director may attend meetings of the GRC as they wish and anyone holding a SMF function may attend to discharge their responsibilities under the Senior Managers Regime.

The Chair of GRC shall be appointed by the Board. In the absence of the committee chair and/or an appointed deputy at a committee meeting, the remaining members present shall elect one of themselves to chair the meeting.



## Secretary

The company secretary, or their nominee, shall act as the secretary of the GRC and will ensure that the GRC receives information in a timely manner to enable full and proper consideration to be given to issues.



## Quorum

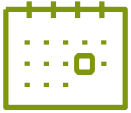
A quorum necessary for the transaction of business shall be any two members.



## Frequency of meetings

The GRC shall meet at least four times per year at appropriate times and otherwise as required.

# Group Risk Committee (GRC) - Terms of Reference



## Notice of meetings

Meetings of the GRC shall be called by the secretary of the committee at the request of the committee chair or any of its members, or at the request of the Chief Risk Officer if they consider it necessary.

Unless otherwise agreed, notice of each meeting confirming the venue, time and date of the meeting, together with an agenda of items to be discussed, shall be forwarded to each member of the GRC and any other person required to attend no later than five working days before the date of the meeting. Supporting papers shall be sent to committee members and to other attendees, as appropriate at the same time.



## Minutes of meeting

The secretary shall minute the proceedings and decisions of all GRC meetings including recording the names of those present and in attendance.

Draft minutes of committee meetings shall be circulated to all members of the committee. Once approved, minutes should be circulated to all members of the board unless, exceptionally, it would be inappropriate to do so.



## Engagement with members

The GRC chair should attend the annual general meeting to answer any member questions on the GRC's activities.



## Duties

The GRC should have oversight of the group as a whole and, unless required otherwise by regulation, carry out the duties below for the Society and its subsidiaries, as appropriate.

### **Risk appetite, tolerance and strategy**

The GRC shall:

Advise the board on the Society's overall risk appetite, tolerance and strategy, and the principal and emerging risks the Society is willing to take in order to achieve its long-term strategic objectives.

The GRC should seek assurance on the risks the Society identifies as those to which the business may be exposed and may include the following:

- Assessment of new initiatives, projects and/or products that have a different risk profile to current Society and/or Group activities;
- Capital;
- Change Delivery risk (if a change being delivered causes an IT or Operational Risk);
- Climate risk;
- Conduct risk;
- Counterparty risk;
- Credit risk;
- Ethical codes;
- Health and safety;
- Insolvency;
- Insurance risk;
- IT operations, including cyber risk;
- Liquidity;

Document classification: L3 - Normal.



## Duties (continued)

### Risk appetite, tolerance and strategy (continued)

- Market Risk;
- Material litigation;
- Model risks
- Operational resilience;
- Operational risk;
- Regulatory and legal risks;
- Regulatory stress testing;
- Reputational risk;
- Risk acceptance by the Society and/or Group;
- Threats to the business model or future performance;
- Transactional risk.

Review and assess the Society's risk appetite and associated stress testing.

Consider and review any matters of relevance escalated to the GRC from the Society's risk sub-committees.

Advise the board of the likelihood and the impact of principal risks materialising, and the management and mitigation of principal risks to reduce the likelihood of their incidence or their impact.

Advise the board on the risk aspects of proposed changes to strategy and strategic transactions, ensuring that a due diligence appraisal (as governed by our procurement and supplier management framework) is undertaken, focussing in particular on implications for the risk appetite, tolerance and strategy of the Society and taking external advice where appropriate and available.

### Internal controls and risk management systems

The GRC shall oversee and seek suitable assurance regarding:

- The risk exposures of the Society, including risk to the Society's business model, solvency and liquidity risks;
- The risk exposures of the Society, including risk to the Society's processes and procedures to manage risk and the internal control framework, including the design, implementation and effectiveness of those systems;
- The ability of the Society's risk management and internal control systems to identify the risk facing the company and enable a robust assessment of principal risks;
- The Society's capability to identify and manage new and emerging risks;
- The effectiveness and relative costs and benefits of particular controls;

### Internal controls and risk management systems (continued)

- The effectiveness of management's processes for monitoring and reviewing the effectiveness of risk management and internal control systems and ensuring corrective action is taken where necessary;
- The Society's ability to reduce the likelihood of principal risks materialising and the impact on this business of risks that do materialise;
- The appropriateness of the Society's values and culture and reward systems for managing risk and internal controls;
- The Chief Risk Officer's right of direct access to the chair of the board and to the GRC.



## Reporting responsibilities

The Chair of the GRC shall report formally to the Board on the Committee's business, at its monthly meetings.

The Chair of the GRC shall provide advice to the Remunerations Committee on any risk weightings to be applied to performance objectives incorporated in the incentive structure for executive remuneration and make recommendations to the remunerations committee on claw-back provisions.

The Chair of GRC shall, at their discretion elevate any matter in the remit of the Committee to the Board where they feel it appropriate to do so.

The committee shall compile a report of its activities to be included within the Society's annual report, describing the work of the committee and shall review and approve the statements to be included in the annual report concerning internal controls and risk management.



## Other matters

The GRC shall:

- Have access to sufficient resources in order to carry out its duties, including access to the company secretariat for advice and assistance as required.
- Be provided with appropriate and timely training, both in the form of an induction programme for new members and on an ongoing basis for all members.
- Give due consideration to all relevant laws and regulations, the provision of the UK Corporate Governance Code and published guidance, and any other applicable rules, as appropriate.
- Oversee any investigation of activities which are within its terms of reference.
- Work and liaise as necessary with all other board committee 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.
- Ensure a periodic evaluation of the committee's performance is carried out.
- 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.



## SMCR

Through our approach to SMCR we allocate prescribed responsibilities (as laid down by the PRA and/or FCA) to individuals (Senior Managers/SMFs). The GRC will collectively assist the Senior Manager Function detailed below in fulfilling the following prescribed and overall/assigned responsibilities:

### Chair of GRC (SMF10):

- Safeguarding the independence of; and oversight of the performance of; the compliance function including the performance of a person approved by the FCA to perform the compliance oversight function on behalf of the Society
- Safeguarding the independence of; and oversight of the performance of the risk function including the performance of a person approved to perform the Chief risk function on behalf of the Society

### Chief Risk Officer (SMF4 / 24):

- Managing the Society's internal stress tests and ensuring the accuracy and timeliness of information provided to the PRA and other regulatory bodies for the purposes of stress testing
- The firm's policies and procedures for countering the risk that the firm might be used to further financial crime
- For identifying and managing risks from climate change
- Managing the Society's performance of its obligations under Outsourcing.



## Authority

The GRC is authorised to:

- Request the attendance of any colleague at a meeting of the GRC and/or seek any information it requires from any colleague of the Society in order to perform its duties.
- Oblige the Society's risk sub-committees to escalate any matters they feel of relevance to the GRC.
- Delegate any matter or matters to another committee or person(s) as it deems appropriate.
- Obtain, at the Society's expense, independent legal or other professional advice on any matter within its terms of reference if it believes it necessary to do so.