Terms of Reference – Governance and Risk Committee

1. Purpose

1.1. The purpose of the Committee is to ensure and provide assurance to the Board that the Society's risk management strategies and governance arrangements are appropriate in respect of the type of business it transacts, the market in which it operates and the regulatory regime by which it is assessed. In particular, the Committee will review, approve and monitor internal risk and compliance strategies and reports. For the purposes of these Terms of Reference any reference to 'the Society' should be deemed to include its subsidiary companies.

1.2. The role of the Committee is to:

1.2.1. Provide oversight and advice to the Board in relation to current and potential future risk exposures of the Society and future risk strategy, including determination of risk appetite and tolerance and the effectiveness of the Society's framework for managing risk.

1.2.2. Promote a risk culture that puts members first within the Society and oversee implementation and maintenance of the Enterprise Risk Management Framework (ERMF).

1.2.3. Review key risk policies and frameworks including risk appetite strategies.

1.2.4. Monitor risks on behalf of the Board via this Committee.

2. Membership

2.1. The Committee shall comprise at least three members. Membership shall include the Chair of the Audit Committee. A majority of members of the Committee shall be independent non-executive directors. Members of the Committee shall be appointed by the Board, on the recommendation of the Nomination Committee in consultation with the Chair of the Governance and Risk Committee.

2.2. The Finance Director shall be a Committee member or in attendance at all meetings. The Chief Risk Officer shall be expected to attend at all meetings.

2.3. Only members of the Committee have the right to attend Committee meetings. However, other individuals including the Chair of the Board, the Chief Executive, other directors, the Chief Actuary, the Head of Compliance, other representatives of the risk function, compliance, and internal and external audit may be invited to attend all or part of any meeting as and when deemed appropriate and necessary by the Board or the Committee.

2.4. Members shall have appropriate knowledge, skills and expertise to fully understand risk appetite and strategy.

2.5. Appointments to the Committee, in respect of Non-Executive Directors, shall be for a period of up to three years, extendable by no more than two additional three-year periods, provided the director still meets the criteria for membership of the Committee and re-election by members.

2.6. The Board shall appoint the Committee Chair who shall be an independent non-executive director. 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. Secretary

3.1. The Company 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 issues.

4. Quorum

The quorum necessary for the transaction of business shall be two independent non-executive director members.

5. Frequency of Meetings

5.1. The Committee shall meet at least four times a year at appropriate times and otherwise as required. Meetings may be held in person, over the telephone or by technology enabled conference. A member of the Committee so participating shall be deemed to be present in person at the meeting and shall be entitled to fully participate and be counted in the quorum accordingly.

5.2. Interim 'specific issue(s)' meetings may be convened, by the Secretary, at the request of the Chair. In circumstances where a decision is required to be made in a timely fashion, the interim meeting may take place by e-mail and shall be valid if the e-mail has been circulated to all members of the Committee and the decision is approved by a quorum.

6. Notice of Meetings

6.1. Meetings of the Committee shall be convened by the Secretary at the request of the Committee Chair or any of its members or at the request of the Chief Risk Officer if they consider a meeting necessary.

6.2. 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, all other non-executive directors 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.

7. Minutes of Meetings

7.1. The Secretary shall minute the proceedings and decisions of all meetings of the Committee, including recording the names of those present and in attendance.

7.2. Draft minutes of Committee meetings shall be circulated within ten working days of the meeting to all members of the Committee. Once approved, minutes shall be circulated to all other members of the Board unless it would be inappropriate to do so in the opinion of the Committee Chair.

7.3. Final signed copies of the minutes of the meetings of the Committee should be maintained for the Society's records.

7.4. Where meetings have taken place by exchange of e-mail, copies of the e-mails shall be included in the minute book as the minutes of the meeting.

8. Annual General Meeting

8.1. The Committee Chair shall attend the Annual General Meeting to answer member questions on the Committee's activities.

9. Responsibilities

The Committee shall carry out the duties below for the Society, its subsidiaries and the group as a whole, as appropriate.

9.1. Internal Controls and Risk Management Systems

The Committee shall:

9.1.1. advise the Board on the Society's overall risk appetite, tolerance and strategy, the principal and emerging risks the Society is willing to take in order to achieve its long-term strategic objectives, taking account of the current and prospective macroeconomic and financial environment and drawing on financial stability assessments such as those published by relevant industry and regulatory authorities including the Bank of England, the Prudential Regulation Authority, the Financial Conduct Authority and other authoritative sources that may be relevant for the Society's risk policies;

9.1.2. oversee and advise the Board on the current risk exposures of the Society and future risk strategy;

9.1.3. in relation to risk assessment and subject to overlap with the Audit Committee:

9.1.3.1. keep under review the Society's overall risk assessment processes that inform the Board's decision making, ensuring both qualitative and quantitative metrics are used;

9.1.3.2. review regularly and approve the parameters used in these measures and the methodology adopted; and

9.1.3.3. set a standard for the accurate and timely monitoring of large exposures and certain risk types of critical importance;

9.1.4. review the Society's ability to identify and manage new risk types;

9.1.5. 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;

9.1.6. before a decision to proceed is taken by the Board, advise the Board on proposed strategic transactions including new ventures, acquisitions or disposals, ensuring that a due diligence appraisal of the proposition is undertaken, focussing in particular on risk aspects and implications for the risk appetite and tolerance of the Society, and taking independent external advice where appropriate and available;

9.1.7. ensure that the material risks facing the Society have been identified and that appropriate arrangements are in place to manage and mitigate those risks effectively;

9.1.8. approve and monitor compliance with the Own Risk and Solvency Assessment (ORSA) policy;

9.1.9. provide oversight of the ORSA process;

9.1.10. provide oversight and challenge in respect of capital management function;

9.1.11. provide oversight and challenge of the design and execution of stress and scenario testing;

9.1.12. review and challenge risk information received from the Society's risk functions to ensure that the Society is not exceeding the risk appetite set by the Board;

9.1.13. review reports on any material breaches of risk limits and the adequacy of proposed action;

9.1.14. keep under review the adequacy and effectiveness of the Society's internal controls and risk management systems and review and approve the statements to be included in the Annual Report concerning internal controls and risk management;

9.1.15. provide qualitative and quantitative advice to the Remuneration Committee on any risk weightings to be applied to performance objectives incorporated in the executive remuneration policies and make recommendations to the Remuneration Committee on clawback provisions and encourage good risk management;

9.1.16. consider and approve the remit of the risk management function and ensure it has adequate resources and appropriate access to information to enable it to perform its function effectively and in accordance with the relevant professional standards. The Committee shall also ensure the function has adequate independence and is free from management and other restrictions;

9.1.17. recommend to the Board the appointment and/or removal of the Chief Risk Officer;

9.1.18. review promptly all reports on the Society from the Chief Risk Officer;

9.1.19. review and monitor management's responsiveness to the findings and recommendations of the Chief Risk Officer;

9.1.20. meet with the Chief Risk Officer at least once a year, without the presence of management;

9.1.21. ensure the Chief Risk Officer shall be given the right of unfettered direct access to the Chair of the Board and to the Committee;

9.1.22. request and review reports on particular aspects of risk management (including but not limited to, conduct risk, operational resilience, information security, data protection, cyber risk, sustainability risk, environment, social and governance risk, and business continuity planning, as the Committee considers appropriate.

9.1.23. keep abreast of both current risk management techniques and theories and any probable or actual changes in the regulatory environment, discuss the impact of the same on the Society and recommend the necessary actions to be taken; and

9.1.24. react to extreme market situations.

9.2. Governance Arrangements and Regulatory Compliance

The Committee shall:

9.2.1. provide oversight of the Society's governance and regulatory compliance arrangements, and its related policies and procedures, and monitor their effectiveness;

9.2.2. keep under review developments and prospective changes in the regulatory environment;

9.2.3. keep under review developments in the AFM Corporate Governance Code and monitor the Society's compliance with the Code's principles and guidance *(with the exception of those that relate to responsibilities delegated specifically to the Nomination and Remuneration Committee)*;

9.2.4. review the Directors' Corporate Governance Report to be included in the Society's Annual Report and Accounts and make a recommendation to the Board regarding its adequacy; and

9.2.5. make recommendations to the Board as to how the Society should engage effectively with its membership.

9.3. Compliance Oversight

The Committee shall:

9.3.1. approve the appointment or termination of appointment of the Head of Compliance;

9.3.2. review and approve the remit of the compliance function and ensure the function has the necessary resources and access to information to enable it to fulfil its mandate and is equipped to perform in accordance with the relevant professional standards. The Committee shall also ensure the function has adequate independence and is free from management and other restrictions;

9.3.3. review and assess the annual compliance plan and monitor progress against the plan;

9.3.4. review regular reports from the Head of Compliance;

9.3.5. review and monitor management's responsiveness to the findings and recommendations of compliance monitoring reports and ensure that the agreed actions are put into effect;

9.3.6. meet the Head of Compliance at least once a year, without the presence of management; and

9.3.7. monitor and review the adequacy and effectiveness of the Society's compliance function.

10. Reporting Responsibilities

10.1. The Committee Chair shall report formally to the Board on its proceedings after each meeting on all matters within its duties and responsibilities.

10.2. The Committee shall make whatever recommendations to the Board it deems appropriate on any area within its remit where action or improvement is needed.

10.3. The Committee shall produce a report on its activities and the Society's risk management and strategy to be included in the Society's Annual Report.

10.4. The Directors' Reports in the Annual Report and Accounts should set out risk management objectives and policies including in relation to financial instruments.

11. Other Matters

The Committee shall:

11.1. have access to sufficient resources in order to carry out its duties, including access to the company secretariat for assistance as required;

11.2. be provided with appropriate and timely training, both in the form of an induction programme for new members and on an on-going basis for all members;

11.3. keep up-to-date on regulatory risk and compliance matters;

11.4. give due consideration to laws and regulations, the provisions of the AFM Corporate Governance Code and any other applicable rules, as appropriate;

11.5. oversee, monitor and provide recommendations to the Boardin promoting the long-term sustainable success of the Society and its stakeholders with regard to environmental, social and governance matters.

11.6. oversee any investigation of activities which are within its terms of reference;

11.7. 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; and

11.8. arrange for periodic 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.

12. Authority

The Committee is authorised to:

12.1. seek any information it requires from any employee or director of the Society in order to perform its duties;

12.2. obtain, at the Society's expense, independent legal, accounting or other professional advice on any matter it believes it necessary to do so;

12.3. to delegate any of its duties as is appropriate to such persons or person as it thinks fit whilst retaining responsibility and oversight for any and all actions taken; and

12.4. request the attendance of any employee at a meeting of the Committee as and when required.