Group Secretariat

Board Risk Committee
Terms of Reference

Approved on:
9 December 2020

RSA Insurance Group plc
20 Fenchurch Street
London EC3M 3AU

RSA Insurance Group plc (the 'Company')

BOARD RISK COMMITTEE (the 'Committee') – TERMS OF REFERENCE

1. Principal Function

1.1 The principal function of the Committee is to support the Board in ensuring the key risks to the Group are identified and understood, effectively managed within risk appetite with regard to the views and interests of its stakeholders and are appropriately reflected in the Internal Model.

1.2 The following specific responsibilities have been delegated to the Committee to assist the Board in discharging its responsibilities:

(A) advising the Board on risk management matters, including solvency needs and compliance matters;

(B) overseeing the risk management arrangements of the Company and the Group;

(C) monitoring the emerging and principal material risks facing the Group, ensuring appropriate arrangements are in place to identify, manage and mitigate risks effectively, and that appropriate levels of capital are held in relation to these risks;

(D) recommending the Group's risk strategy and risk appetite;

(E) approval of the Risk Management Plan;

(F) reviewing the outputs of the ORSA process, the internal model and the conclusions of model validation, making recommendations to the Board on capital adequacy and the Group ORSA Report; and

(G) oversight of the risk and compliance function and risk governance, including recommending the System of Governance to the Board.

1.3 In undertaking its duties and responsibilities, the Committee should, where appropriate, be mindful of the views and interests of the Company's shareholders and its stakeholders particularly those of the customers and the need to deliver good customer outcomes.

2. Membership

2.1 The Committee members shall be appointed by the Board on the recommendation of the Nomination Committee and in consultation with the Chair of the Committee. The Committee shall comprise at least three members, all of whom shall be independent Non-Executive Directors. Membership shall include at least one member of the Group Audit Committee and one member of the Group Remuneration Committee.

2.2 The Chairman of the Committee shall be an independent Non-Executive Director.

2.3 Care shall be taken to minimise the risk of any conflict of interest that could arise.

2.4 The Board shall appoint the Committee Chairman on the recommendation of the Nomination Committee and determine the period for which they shall hold office. In the absence of the Committee Chairman, the remaining members present shall elect one of their number to chair the meeting.

3. Attendance

3.1 Only Committee members have the right to attend Committee meetings. The Committee Chairman may invite any directors, or other employees of the Group or professional advisers to attend all or part of any meeting as and when appropriate.

3.2 The Group Chief Financial Officer, Group Chief Risk Officer and Group Chief Compliance Officer shall be expected to attend Committee meetings. For the avoidance of doubt, they are not members of the Committee.

3.3 The Group Chief Underwriting Officer, Group Chief Legal Officer and Company Secretary, Group Chief Auditor, Regional Chief Risk Officers and Group level Risk Directors may attend meetings at the Committee's invitation.

3.4 The Company's external auditor may request to attend Committee meetings and the Committee Chairman may authorise this.

3.5 If a Committee member is unable to attend due to absence, illness or any other cause, the Chairman of the Committee may appoint an independent Non-Executive Director to serve as an alternate member, maintaining the quorum set out in paragraph 5.1 below.

4. Secretary

4.1 The Group Chief Legal Officer and Company Secretary or his or her duly appointed nominee shall act as the Secretary of the Committee.

5. Quorum

5.1 The quorum necessary for the transaction of business shall be any two members of the Committee. Attendance by an alternate shall count towards the quorum.

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 The Committee may meet for the despatch of business, adjourn and otherwise regulate meetings as they think fit. Without prejudice to the foregoing, all members of the Committee may participate in a meeting of the Committee by means of a conference telephone or any communication equipment which allows all persons participating in the meeting to hear each other. 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.

6. Frequency of Meetings

6.1 The Committee shall meet at least four times each year at appropriate times in the reporting and audit cycle and at such other times as otherwise required.

6.2 Each year, the Committee shall have at least one meeting, or part thereof, with the Group Chief Risk Officer and the Group Chief Compliance Officer in the absence of other members of executive management. In addition, the Group Chief Risk Officer and the Group Chief Compliance Officer shall be offered direct access to the Committee Chairman and, where necessary, the Chairman of the Board.

7. Notice of Meetings

7.1 Meetings of the Committee shall be convened by the Secretary to the Committee at the request of the Chair of the Committee, any of its members or the Group Chief Risk Officer. Meetings can also be requested by management, or the external or internal auditors if they consider it necessary.

7.2 Unless otherwise agreed, notice of each meeting confirming the venue, date and time together with an agenda of items to be discussed and supporting papers, shall be forwarded to each member of the Committee and to other attendees as appropriate prior to the date of the meeting.

8. Minutes of Meetings

8.1 The Secretary shall minute the proceedings and decisions of all Committee meetings, including recording the names of those present and in attendance. The Secretary shall also minute the proceedings and resolutions of any private meeting between the Non-Executive Directors, the internal auditors and the external auditors or the Group Chief Risk Officer where executive management are not present, at the discretion of the Committee Chairman.

8.2 The members of the Committee shall, at the beginning of each meeting, declare the existence of any conflicts of interest arising and the Secretary shall minute them accordingly.

8.3 Draft minutes of Committee meetings shall be circulated promptly to the Committee Chairman and once agreed to all members of the Committee.

8.4 Once approved, minutes of Committee meetings shall be circulated to all members of the Board unless it would be inappropriate to do so.

9. Annual General Meeting

9.1 The Committee Chairman shall attend the Annual General Meeting and respond to any shareholder questions on the Committee's activities and responsibilities.

10. Responsibilities

The Committee shall carry out the duties below for the Company, subsidiary undertakings and the Group as a whole, as appropriate. The Committee's responsibilities shall include, but shall not be limited to:

10.1 Solvency Needs and Own Risk Solvency Assessment (ORSA):

(A) Reviewing, at least annually, the outputs of the internal model, including but not exclusively Solvency II SCR, as recommended by the Internal Model Governance Committee, to include a review of the overall assumptions, results, model changes and the conclusions of the internal model validation process and if satisfied, make recommendations to the Board; and

(B) Overseeing the Group ORSA process and reviewing the ORSA report for recommendation to the Board for approval.

10.2 Risk Management, Risk Appetite and Risk Profile:

(A) Maintaining oversight of the effectiveness of the risk management system, including Compliance in respect of customer and conduct risks;

(B) Considering and approving the Group's overall risk strategy and framework of risk appetite and risk limits for recommendation to the Board for approval at least annually;

(C) Approval of the Risk Management Plan at least annually to review functional priorities and Technical, Financial and Operational Assurance Plans, including Conduct Assurance Plans;

(D) In each committee meeting, with the benefit of input from the Regional Risk Directors, ensuring the material risks facing the Group (including key customer related risks and horizon scanning outputs) have been identified, that the risk profile adequately represents any significant issues relating to the Group's control environment and that mitigating actions are in place;

(E) As appropriate, advising the Board on 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;

(F) Reviewing the risk appetite capital adequacy assessment and where necessary approve actions to bring capital within appetite on a regular basis;

(G) In each committee meeting overseeing and challenging the management of conduct risk and ensuring that appropriate action is being taken to address risks or issues impacting achievement of good customer outcomes;

(H) Considering the output from deep dive reviews performed for key risks, including an assessment of the appropriateness of mitigating actions to maintain risks within appetite;

(I) Review reports on any material breaches of risk limits, noting where these breaches are linked to policy gaps and actual or potential impact to customers, together with assessing adequacy and timing of proposed actions;

(J) Regularly review and monitor emerging risks which may have a future material impact on the Group or its stakeholders, including customers;

(K) Regularly reviewing Stress and Scenario Testing results and actions proposed or taken to address any identified risks and provide input into the selection of appropriate stress and scenario tests;

(L) Reviewing the effective management of financial risks from climate change, ensuring they are integrated into the wider risk management system;

(M) Reviewing promptly all material reports from the Group Chief Risk Officer, which will include a summary of key messages from other relevant committees, especially Regional Risk and Control Committees and Customer Committees (minutes from the regional Risk and Control Committees are available to all Committee members on request);

(N) Reviewing and monitoring management's responsiveness to the findings and recommendations of the Group Chief Risk Officer;

(O) Overseeing the appropriateness of the Group's values and culture and reward systems for managing risk and internal controls, and the extent to which the culture and values are embedded at all levels of the Group;

(P) Providing insights to the Remuneration Committee to enable proper consideration of risk in remuneration decisions for the Group and the remuneration of employed executives who are members of the Board (the 'Executive Directors') and other senior executives; and

(Q) Advising the Board, at their request, on changes to strategy and strategic transactions including significant acquisitions or disposals, ensuring that adequate due diligence and assessment has been performed in consideration of the business and its customers. In particular, reviewing risk aspects of the transaction and the impact on the Group's risk appetite and tolerance.

10.3 Compliance:

(A) Considering and approving the mandate and role of the Group Risk and Compliance Function on an annual basis and ensuring that the function is independent, adequately resourced and has appropriate access to information to enable it to perform its function effectively and in accordance with relevant professional standards;

(B) Review and approving the annual Group Compliance Plan and any changes to the Plan;

(C) Oversight of the Group's compliance with legal and regulatory requirements

of each territory in which the Group transacts business within the scope of the Compliance Function;

(D) Reviewing regular reports from the Group Chief Compliance Officer on the outcome of assurance reviews, and other compliance issues and activities throughout the Group; and

(E) In relation to Data Protection, in line with the General Data Protection Regulation, receiving a report at least annually on the Group's systems and controls for the protection and management of personal data, and approving the Personal Data Protection Assurance Framework.

10.4 System of Governance:

(A) Considering and approving the Group's System of Governance for recommendation to the Board for approval at least annually, with regular assurance reporting on the Internal Control System being reviewed by the Committee or the Group Audit Committee as appropriate;

(B) Regularly reviewing the Group's risk management system;

(C) Reviewing and approving the adoption of new Group Policies, material changes to existing Group Policies or their termination/change of status on recommendation of the Control and Governance Advisory Committee ("CGAC");

(D) Considering and approving the Line 2 Charter on an annual basis and ensuring that the function is independent, adequately resourced and has appropriate access to information to enable it to perform its function effectively and in accordance with relevant professional standards; and

(E) Reviewing any recommendation of the Executive Directors on the appointment or removal of the Group Chief Risk Officer and making appropriate recommendations to the Board.

11. Reporting Responsibilities

11.1 The Committee Chairman shall report formally to the Board on its proceedings after each meeting.

11.2 The Committee shall:

(A) at least once a year, review its own performance, constitution and terms of reference to ensure it is operating effectively, and recommend any changes it considers necessary to the Board;

(B) the Committee shall make whatever recommendations to the Board it deems appropriate on any area within its remit where action or improvement is needed;

(C) produce a report as part of the Company's Annual Report and Accounts describing the Committee's activities during the relevant financial year, including details of any issues that could not be resolved between the

Committee and the Board and in compliance with relevant law, regulation and best practice; and

(D) make available its terms of reference in accordance with the provisions and recommendations contained within the UK Corporate Governance Code.

12. Other matters

12.1 The Committee shall:

(A) utilise common memberships and work collaboratively with other Group committees including, but not limited to, the Audit Committee to address any overlapping themes arising from time to time;

(B) have access to sufficient resources in order to carry out its duties, including access to the Group's Secretariat for assistance as required;

(C) 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;

(D) give due consideration to the requirements of the UK Listing Authority's Listing Rules, Disclosure and Transparency Rules, Prospectus Rules, the provisions of the Code and any other relevant laws or regulations in force from time to time;

13. Authority

13.1 The Committee is authorised by the Board to:

(A) investigate any activity within its terms of reference;

(B) seek any information it reasonably requires in order to effectively perform its duties;

(C) obtain, at the Company's expense, independent legal or other professional advice on any matters within its terms of reference;

(D) call any member of staff to attend a meeting of the Committee as and when required; and

(E) 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.

13.2 Authority is delegated to the Control and Governance Advisory Committee and the Internal Model Governance Committee in line with their Terms of Reference as approved by the Committee.