



Santam Group Risk Committee Charter

SANTAM GROUP RISK COMMITTEE CHARTER

1. Constitution

- 1.1 The Risk Committee (the Committee) is constituted as a Committee of the Board of Directors (the Board) of Santam Limited (the Company).
- 1.2 The duties and responsibilities of the members of the Committee are in addition to those as members of the Board.
- 1.3 The deliberations of the Committee do not reduce the individual and collective responsibilities of Board members in regard to their fiduciary duties and responsibilities, and they must continue to exercise due care and judgement in accordance with their statutory obligations.
- 1.4 This Charter is subject to the provisions of the Companies Act, the Company's Articles of Association and any other applicable law or regulatory provision (including JSE listing requirements).
- 1.5 The Committee should assist the Board in carrying out its responsibilities regarding governance, compliance and risk management. The Committee does not perform any management functions or assume any management responsibilities.
- 1.6 The membership, resources, responsibilities and authorities (composition, functions, and operation) of the Committee to perform its role effectively, are stipulated in this Charter. The Committee is constituted in terms of the requirements of sound corporate governance practices and operates within that framework.
- 1.7 When reference is made to the "Company" is it implied that it refers to Santam Ltd, the insurance licenced entity, while the "Group" refers to Santam Ltd as well as all material subsidiaries, including the licensed subsidiaries.
- 1.8 When reference is made to licensed entities, it refers to entities that are licensed in terms of the Short-term Insurance Act, as amended from time to time.
- 1.9 The Risk Committee will satisfy itself as to the adequacy of the governance, compliance and risk management structures and processes of all material associates.

2. Purpose of the Charter

- 2.1 The purpose of the Charter is to set out the Committee's role and responsibilities as well as the requirements for its composition and meeting procedures.

3. Composition

- 3.1 The Committee should comprise of a minimum of three directors. Membership of the Risk Committee could include executive and non-executive directors, with the majority members being non-executive directors.
- 3.2 Members of this Committee and its Chairman are nominated by the Board.
- 3.3 The composition of the Committee must ensure objective oversight and decision making.
- 3.4 The Committee must have an appropriate mix of members to ensure an adequate spread and level of knowledge, experience, skills and expertise to fulfil their duties.

-
- 3.5 The Board shall appoint a Chairman from the non-executive, independent members of the Committee and determine the period for which he or she shall hold office.
 - 3.6 The members of the Audit Committee will be members of this Committee.
 - 3.7 The Board shall have the power at any time to remove any members from the Committee and to fill any vacancies created by such removal.

4. The role of the Committee

The primary function of the Committee is to assist the Board in fulfilling its responsibility for governance (from a risk and control perspective), compliance, and risk management. The Committee has an independent role, operating as an oversight function and a maker of recommendations to the Board for its consideration and final approval. The role of the Committee is to assist the Board in ensuring that:-

- 4.1 The Group implements an adequate and effective system for governance, compliance and risk management that enhances the Group's ability to achieve its strategic objectives whilst protecting legitimate stakeholders and ensuring adequate protection of policyholders.
- 4.2 The governance, compliance and risk management system implemented at subsidiary level (including licensed entities) is proportionate to the nature, scale and complexity of the relevant businesses and in relation to the Group.
- 4.3 The maturity and effectiveness of the governance, compliance and risk management processes and activities are continuously monitored, maintained and improved as required.
- 4.4 The overall risk profile, including significant risks faced by the Group, are monitored and reviewed and the responses to address these key risks are appropriately defined and resolved by management.
- 4.5 The disclosure regarding governance, compliance and risk is comprehensive, timely and relevant.
- 4.6 There is adequate oversight over the Own Risk & Solvency Assessment (ORSA) and Internal Model processes from a solo license and Group perspective, where applicable.
- 4.7 Conduct of business risks are monitored and mitigated by the achievement of the outcomes of Treating Customers Fairly (TCF) from a solo license and Group perspective in line with the Santam Group Risk Appetite.

5. Responsibilities

Management is accountable to the Board for designing, implementing and monitoring the process of governance, compliance and risk management, including its integration into the day-to-day activities of the Group. The Committee must perform all the functions as is necessary to fulfil its role as stated above including the following:

- 5.1 Providing oversight and monitoring of the design and implementation of the governance, risk management and compliance systems. This includes the following:
 - 5.1.1 providing oversight over the philosophy, strategy, framework, policies and plans for governance, compliance and risk management to ensure systematic, disciplined approaches are developed and implemented.

-
- 5.1.2 reviewing and recommending (if required) any changes to the philosophy, strategy, policies and plans for approval to the Board.
 - 5.1.3 expressing a formal opinion to the Board on the adequacy and efficiency of the system and process of governance, compliance and risk management.
 - 5.1.4 introducing such measures as may serve to enhance the adequacy and efficiency of the governance, compliance and risk management system
 - 5.2 Providing oversight over the internal control systems as implemented by management to reasonably ensure, from a control perspective, that the business is being operated and consistently aligned with:
 - 5.2.1 the Board's strategy;
 - 5.2.2 agreed business objectives,
 - 5.2.3 agreed policies and processes,
 - 5.2.4 customer fairness and conduct related risks, and
 - 5.2.5 applicable laws and regulations and relevant industry Codes
 - 5.3 Assisting the board in identifying and regularly monitoring all material risks and key indicators to ensure that its decision-making capability and accuracy of its reporting is maintained at a high level.
 - 5.4 Assisting the board in the identification of the concentration of the various risks to which the insurer is exposed.
 - 5.5 Ensuring the establishment of independent control functions¹ as required by the Regulator with access to the board of directors and all relevant employees and information. The risk, compliance and actuarial control functions reports and is accountable to the risk committee as agreed within their respective charters.
 - 5.6 The appointment, performance assessment, remuneration, disciplining and dismissal of the head of control functions (risk, compliance and actuarial) must be done with the approval of, or after consultation with the risk committee.
 - 5.7 Monitoring the performance of each control function and ensuring that the heads of the various control functions at all times meet the relevant "fit and proper" requirements as determined by the Regulator to facilitate the sound and prudent management of the Group.
 - 5.8 Ensuring that independent reviews are performed on all the control functions at least every three years by internal audit or an objective external reviewer.
 - 5.9 Monitoring and recommending to the Board the levels of risk appetite and monitoring that those risks are managed within the levels of tolerance as approved by the Board.
 - 5.10 Providing oversight that the relevant executive committees of the businesses and business units within the Group have a formal process for the on-going management of risk covering all the relevant risk categories as defined within the Risk Universe.
 - 5.11 Ensuring that frameworks and methodologies are implemented to increase the probability of anticipating unpredictable risks (also referred to as new and emerging risks).

¹ Control function within a governance framework, means the risk management function, the compliance function, the actuarial function and internal audit function. For purposes of this charter, internal audit is excluded as this will be covered in the Audit Committee charter.

-
- 5.12 Facilitating and promoting communication, through reporting structures, regarding matters around the evaluation of the adequacy and efficiency of the governance, risk and compliance management systems (as highlighted in 5.1.3-4 above) or any other related matter, between the board and managing executives. Also to liaise closely with the Audit Committee and the Executive Risk Forum (ERF) to exchange information relevant to risk.
- 5.13 Reviewing reports concerning governance, compliance and risk management that are to be included in the integrated report.
- 5.14 Reviewing the internal model governance and validation framework to support the Board in its overall responsibility with regards to the internal model. The responsibilities of the Risk Committee include:-
- 5.14.1 Reviewing and recommending to the Board for approval the application to use the IM and any changes to the IM in terms Santam's IM Change Policy;
 - 5.14.2 Deciding the roles and responsibilities for internal model governance;
 - 5.14.3 Deciding the strategic direction of the model and hence any changes to the model;
 - 5.14.4 Agreeing major changes in advance of the change being made;
 - 5.14.5 Aligning the model design and operations with the undertaking's risk profile and operations;
 - 5.14.6 Ensuring that there are sufficient resources to develop, monitor and maintain the model;
 - 5.14.7 Monitoring on-going compliance with the requirements for internal model approval and informing the supervisory authorities if the model ceases to comply;
 - 5.14.8 Ensuring there are adequate independent review procedures in place around the internal model design, operation and validation;
 - 5.14.9 Ensuring that outputs are aligned with use – i.e. that the management information produced by the model assists in decisions made at Board level; and
 - 5.14.10 Should the internal model cease to comply with the requirements for approval, the Board or Senior Management must ensure that a plan to restore compliance is developed or assess the non-compliance as immaterial.
- 5.15 Reviewing and discussing the Group's IT Governance Charter to ensure that it is appropriate, aligned and supports the Group's strategy and risk appetite. Specifically in terms of IT Governance that the principles should align to the Sanlam Group wide IT Governance principles, which per definition are also aligned to King III.
- 5.16 Reviewing the company secretarial reports including the review of the D&O and the JSE Compliance report.
- 5.17 Reviewing both the Group and the Company's Own Risk & Solvency Assessment (ORSA) process to support the Board in its overall responsibility to assess its risk management framework as well as the solvency requirements and the own funds available to meet these requirements. In particular:-
- 5.17.1 Assessing the adequacy of the current and projected future solvency position
 - 5.17.2 Considering the impact of any business strategy, including large and complex transactions on the current and future solvency position
 - 5.17.3 Reporting to the Board on any circumstances that are likely to significantly impact Santam's current or projected future solvency position
 - 5.17.4 Ensuring that the ORSA requirements are embedded in the business and decision making processes
 - 5.17.5 The Risk Committee should also, through direct review and challenge and through reliance on the governance process, conclude on the accuracy and completeness of the ORSA calculations, assumptions and data used as input to the ORSA

-
- 5.18 Providing oversight over outsourcing activities to support the Santam Board in its overall responsibility of any material functions, management functions, control functions or activities that have been / are planned to be outsourced by / within the Santam Group. The following should be included at the relevant Board level within the Group:-
- 5.18.1 Agreeing on outsourcing strategies and deciding on business activities of a material nature to be outsourced.
 - 5.18.2 Laying down appropriate approval authorities for material outsourcing depending on risks and materiality (aligned to the relevant Delegation of Authority document).
 - 5.18.3 Recommending the approval of an Outsourcing Policy and subsequent annual revisions of the policy.
 - 5.18.4 Receiving reports from Executive Management to evaluate the risks of all material existing and prospective outsourcing and the contracts that apply to such arrangements.
 - 5.18.5 Evaluating the annual feedback on the management of material outsource business services which should include reporting on any outsourced business services considered material from a regulatory perspective.
- 5.19 At a Group level the maintenance of a central register of outsourced functions, including intergroup, and which needs to be presented to the Risk Committee on annually basis or as required.
- 5.20 Monitoring that business operations are aligned with TCF outcomes across the Group and that the risks associated with these outcomes are appropriately managed within the levels of tolerance and appetite as approved by the Board.

6. Authority of the Committee and resources available to it

The Committee acts in terms of the delegated authority of the Board as recorded in this Charter. The Committee, in fulfilling its duties, is authorised to do the following:

- 6.1 Account to the Board on the Committee's activities and make recommendations to the Board concerning matters arising from the above responsibilities.
- 6.2 Make recommendations to the Audit Committee on matters relating to the adoption of the annual and interim financial statements and any other relevant risk matters arising from the above responsibilities.
- 6.3 Investigate any activity within its Charter.
- 6.4 At its discretion, require other employees or management of the Company (which includes subsidiaries) to attend meetings or parts of meetings.
- 6.5 Call upon the chairman of any other Board Committees within the Santam Group, any of the executive directors, officers or company secretary to provide it with information.
- 6.6 Consult with and request information from any employee. All employees shall be required to co-operate with any request made by the Committee in the course of the discharge of its duties as set out in this Charter.
- 6.7 Require periodic briefings and meetings with management, internal and external auditors on issues necessary to enable the Committee to perform its stated functions.
- 6.8 Have reasonable access to the company's records, facilities and any other resources necessary to discharge its duties and responsibilities.

- 6.9 Obtain independent outside professional advice to assist with the execution of its duties, at the Company's cost, subject to following a Board approved process.

7. Proceedings

7.1 Frequency

- 7.1.1 The Committee must hold sufficient scheduled meetings to discharge all its duties as set out in the Charter, but will convene on a quarterly basis at a minimum.
- 7.1.2 Meetings in addition to those scheduled may, with approval of the Chairman, be held at the request of the Chief Executive Officer, the Chief Risk Officer, Head: Enterprise Risk Management, Head: Financial Risk Management, the Compliance Officer or other members of senior management or at the instance of the Board.
- 7.1.3 The chairman of the Committee may meet with the Chief Executive Officer, any of the heads of the Internal Control functions and/or the Company Secretary prior to a Committee meeting to discuss important issues and agree on the agenda.

7.2 Attendance

- 7.2.1 The Chairman of the Investment Committee, the Chief Executive Officer, the Chief Risk Officer, Executive Head of Finance, Executive Head of Underwriting Risk and Reinsurance, the Executive Head of Information and Information Technology, Head: Internal Audit, Head: Enterprise Risk Management (ERM), Head: Financial Risk Management (FRM) and the Compliance Officer will be invited to attend meetings of the Committee (should they not already be members). Other members of executive management, assurance providers may be in attendance at Committee meetings, but by invitation only. Invitees may not vote.
- 7.2.2 The chairman of the Financial Reporting Review Committee (FRRC) of all the insurance entities within the Group shall also be invited to attend meeting of the Committee.
- 7.2.3 Committee members must attend all scheduled meetings of the Committee, including meetings called on an ad hoc-basis for special matters, unless a prior apology has been submitted to the Chairman or Company Secretary.
- 7.2.4 The Company Secretary is the secretary to this Committee.
- 7.2.5 If the nominated Chairman of the Committee is absent from a meeting, the members present shall elect one of the members present to act as chairman.
- 7.2.6 Members of the Board of Directors are welcome to attend a Committee meeting at any time. Notice should however be given in advance to the secretary of the Committee to enable the proper distribution of documentation.

7.3 Agenda and minutes

- 7.3.1 The Committee must establish an annual work plan for each year to ensure that all relevant matters are covered by the agendas of the meetings planned for the year. The proposed annual plan is attached as **Addendum A**.
- 7.3.2 A detailed agenda, with supporting documentation, must be circulated, at least one week prior to each meeting, to members of the Committee and other invitees.
- 7.3.3 The minutes must be completed as soon as possible after the meeting and circulated to the chairman and members of the Committee for review thereof.
- 7.3.4 Minutes and meeting documentation should be available for review to all members of the Board of Directors.
- 7.3.5 Minutes of the latest (FRRC) meeting of the licenced entities should be included.

7.4 Quorum

- 7.4.1 A representative quorum for meetings is a majority of the members.
- 7.4.2 Individuals in attendance at Committee meetings by invitation may participate in discussions but do not form part of the quorum for Committee meetings, and may not vote.

8. Remuneration

Having regard to the functions performed by the members of the Committee in addition to their functions as directors and in relation to the activities of the Committee and pursuant to the specific power conferred upon the Board by the articles of association of the company, members of the Committee shall be paid such remuneration in respect of their appointment as shall be fixed by the Board and approved by shareholders.

9. Evaluation

The Board must perform an evaluation of the effectiveness of the Committee every year.

10. Approval of this Charter

This Charter was approved by the Board of Directors on 27 November 2019 and will be due for review annually.

Risk Committee annual plan:

During the February and August meetings, the focus of the Risk Committee and Audit Committee will be on financial reporting. The focus will shift to governance, compliance and risk management and control environment issues during the May and November meetings. Material issues relating to governance, compliance, risk management and the control environment will be included on the agenda of other meetings if required.

Notes:

* - Refer to Santam Ltd (the licence) as well as all material subsidiaries

	Feb	May	Aug	Nov
<u>RISK COMMITTEE – GENERAL</u>				
• Executive session with Enterprise Risk & Compliance Management (ERCM) & Financial Risk Management (FRM)	X	X	X	X
• Annual Risk Committee assessments (includes review by Board)				X
• Review of Risk Committee Charter				X
• Report to Board of Directors on Risk Committee assessment				X
• Assessment of Risk Committee member training needs	As needed			
• Review of the annual governance, compliance and risk management plan				X
• Define risk appetite, escalation process and define reporting requirements				X
• Consider adequacy of management information to the Board	X	X	X	X
• Executive session of Committee members (no attendees)				X
• Express formal opinion to the Board on adequacy and effectiveness of governance, compliance and risk management and review reporting included in annual integrated report	X			
• Annual appraisal of the control functions (risk, compliance and Financial Risk Management/actuarial)				X
• Approve/Consult on the appointment, performance assessment, remuneration, disciplining and dismissal of the head of each control function (other than the head of the internal audit function)	As needed			
• Review independence, budget & staffing of control functions (compliance / risk / actuarial)				X
<u>GOVERNANCE</u>				
• Review of Corporate Governance Policy and Framework*		X		
• Review of Corporate Governance report *		X		X
• Review of the IT Charter and maturity against the IT Charter*				X
• Review control functions (risk, compliance and actuarial) charters		X		
• Review the heads of control functions against “Fit & Proper” requirements (Risk Management, Compliance and Actuarial function)				X
<u>COMPLIANCE</u>				

	Feb	May	Aug	Nov
<ul style="list-style-type: none"> Review the Compliance function Charter, Framework and the Compliance Universe * 		X		
<ul style="list-style-type: none"> Review Compliance Policy * 		X		
<ul style="list-style-type: none"> Review Compliance Officer Report against the compliance universe *(including assessment of key compliance and conduct risks and actions to address these) 	X	X	X	X
<ul style="list-style-type: none"> Review Compliance maturity assessment 				X
<ul style="list-style-type: none"> Review the Compliance strategy, annual plan, resourcing and progress against plan 				X
<ul style="list-style-type: none"> Review Competition Law Risk regarding the measures implemented by management 		X		
RISK MANAGEMENT				
<ul style="list-style-type: none"> Review and recommend for approval to the board the Company’s Risk Management Policies including the following*: <ul style="list-style-type: none"> Overall risk management policy and following distinct component policies: <ul style="list-style-type: none"> Investment Policy Re-insurance and risk mitigation Policy Fit and proper policy Remuneration policy (as reviewed by the Remuneration committee) – review to ensure appropriateness in light of “unnecessary risk taking”, inclusion of relevant claw backs and disclosure requirements Underwriting risk management policy Operational risk management policy IT Governance policy Insurance fraud risk management policy Internal Controls Policy Outsourcing Policy 		X		X
<ul style="list-style-type: none"> Review of the internal control system 				
<ul style="list-style-type: none"> Review Risk Universe * 		X		
<ul style="list-style-type: none"> Review Risk Profile including new and emerging risks* 	X	X	X	X
<ul style="list-style-type: none"> 				
<ul style="list-style-type: none"> Review performance against the Risk Appetite criteria and monitor that risks are managed within tolerance levels * 	X	X	X	X
<ul style="list-style-type: none"> Discuss assurance and oversight over material risk areas (as discussed in the combined assurance model) 				X
<ul style="list-style-type: none"> Presentations by risk owners and EXCO 	On request			
<ul style="list-style-type: none"> Review of adequacy and effectiveness of risk management process * 	Independent assurance provided by Internal Audit at agreed intervals			
<ul style="list-style-type: none"> Approve the strategy, plan and review progress and resourcing* 				X

	Feb	May	Aug	Nov
• Review significant investigations		X		X
• Review Risk Management Maturity Assessment				X
<u>Reinsurance</u>				
• Review reinsurance strategy				X
<u>Internal Model & ORSA process</u>				
• Review Capital Status Report	X	X	X	X
• Review ORSA process and report* ²		X		
• Review Internal Model compliance and major changes	X	X	X	X
• Review Internal Model Validation Report	X	X ⁱ	X	X
• Review governance and oversight over internal model		X		
<u>Outsourcing</u>				
• Review Outsourcing Register & associated risks				X
<u>Business Continuity Planning</u>				
• Business continuity management - update on the readiness of the business to continue operating during and after operations *		X		X
• Review Business Continuity Maturity Assessment *				X
<u>Company Secretarial Reports</u>				
• D&O Insurance *				X

ⁱ At least annually or as required by the Internal Model Change Policy (following material changes to the internal model).

² At least annually or as required by the ORSA Policy (following material changes to the risk profile)