

---

**SANLAM KENYA PLC**

**ENTERPRISE RISK MANAGEMENT (ERM) POLICY**

---

<b>SANLAM KENYA PLC ENTERPRISE RISK MANAGEMENT (ERM) POLICY</b>	
<b>Type of Policy:</b>	Sanlam Kenya Plc
<b>Entities subject to this Policy:</b>	Sanlam Kenya Plc Group companies
<b>Governance Area Addressed:</b>	Risk Management
<b>Approving Authority:</b>	Sanlam Kenya Plc Board
<b>Exco Sponsor:</b>	Sanlam Kenya Plc Head of Risk and Compliance
<b>Responsible Person:</b>	Sanlam Kenya Plc Head of Risk and Compliance
<b>Date of First Approval:</b>	2023
<b>Frequency of review or update:</b>	Annual review
<b>Date of next review</b>	2024
<b>Version number:</b>	2023
<b>Related Policies</b>	Sanlam Kenya Plc ERM Framework Sanlam Kenya Plc Risk Escalation Policy

## 1. Policy purpose

The purpose of the policy is to provide a general framework and guidance in terms of risk management applicable to all Sanlam Kenya Plc entities and businesses.

## 2. Objectives of Enterprise Risk Management

The primary objective of Sanlam Kenya Plc's Enterprise Risk Management approach is to develop a holistic, portfolio view of the most significant risks to the achievement of Sanlam Kenya Plc's most important objectives, starting with its primary objective of optimising the return on Group Equity Value and to protect and grow shareholder value within the board approved Risk Appetite.

Successful implementation of the approach will also achieve other objectives such as:

- 2.1 Safeguarding Sanlam Kenya Plc's assets (including information) and investments.
- 2.2 Supporting strategic business goals.
- 2.3 Supporting business sustainability under normal and adverse operating conditions.
- 2.4 Responsible behaviour towards all stakeholders having a legitimate interest in Sanlam Kenya Plc, including customers; and
- 2.5 Providing reliable information about risks affecting the achievement of Sanlam Kenya Plc's core objectives.

## 3. Key definitions

### 3.1. Definition of Enterprise Risk Management

Enterprise Risk Management (ERM) is a high-level over-arching framework aimed at ensuring that:

- 3.1.1 All risks which could jeopardise/enhance achievement of Sanlam Kenya Plc's strategic goals are identified.
- 3.1.2 Appropriate structures, policies, procedures, and practices are in place to manage these risks.
- 3.1.3 Providing a holistic, portfolio view of the Sanlam Kenya Plc's most significant risks, taking a portfolio view of risk.
- 3.1.4 Sufficient organisational resources are applied to, and corporate culture is fully supportive of, the effective implementation of these structures, policies, procedures, and practices.
- 3.1.5 Sanlam Kenya Plc's risks are managed in accordance with the above, in line with the board approved Risk Appetite.

### 3.2. Definition of risk

Risk is inherent in doing business and includes all the uncertain consequences of business activities that could prevent Sanlam Kenya Plc achieving its strategic goals.

Sanlam Kenya Plc's risk management process is aimed at managing each of the three elements of risk i.e. opportunity, hazard, and uncertainty, defined as follows:

- 3.2.1 Opportunity  
Managing risk on the upside as an "offensive" function; focusing on actions taken by management to increase the probability of success and decrease the probability of failure. In practical terms, this would involve identifying outcomes that have exceeded a previously defined benchmark and could allow for further exploitation.
- 3.2.2 Hazard  
Managing risk on the downside as a "defensive" function; focusing on the prevention or mitigation of actions that can generate losses.
- 3.2.3 Uncertainty  
Managing the variability associated with risk, focusing on achieving overall financial performance that falls within a defined acceptable range.

## 4. Implementation of the policy

### 4.1. Scope/applicability of policy

This policy document applies to all **Sanlam Kenya Plc Group companies** consisting of direct or indirectly held: (a) wholly owned subsidiary investments; and (b) other consolidated investments (partially owned subsidiaries and potentially associate investments) in which Sanlam Kenya Plc has a long-term strategic interest and has either equity control or material influence that requires consolidation of such entity:

- 4.1.1 Each Sanlam Kenya Plc Group company's risk management process should relate to all businesses in its sphere of responsibility irrespective of geographical location.
- 4.1.2 The risk management policy should clearly define risk management responsibility at Sanlam Kenya Plc level. Any businesses that are excluded and reporting via an independent structure should be separately identified. Exclusion of specific businesses and separate reporting are subject to final approval by the Sanlam Kenya Plc CEO after considering the motivation and support presented by the Sanlam Kenya Plc Group company's Actuarial, Audit and Risk Committee, the Sanlam Kenya Plc Functionary responsible for the particular area and the necessary approvals required from Sanlam. All approved deviations must be filed with the Sanlam Kenya Plc Group Company Secretary.
- 4.1.3 Each business is responsible for the risks related to its outsourced functions unless it delegates this to a central support function, in which case the latter must establish a risk management policy and liaise with the Sanlam Kenya Plc Head of Risk and Compliance.

The other non-controlled **Sanlam Kenya Plc Associates, if any** (essentially long-term strategic investments) are not included in the detailed policy requirements of this document. The responsible Sanlam Kenya Plc Executives, as well as the Sanlam Kenya Plc board representatives are, however, required to ensure that Sanlam Kenya Plc maintains an acceptable level of influence to be able to secure the application of similar or appropriate alternative governance processes and practices in such entities. The Sanlam Kenya Plc Executives must ensure there are appropriate internal risk management, controls and governance structures and processes in place. The Sanlam Kenya Plc Executives must further ensure that associated risk reporting and escalation takes place, and that adequate Sanlam Kenya Plc representation is present at the various Risk and Audit Committee(s).

The detailed definitions and other governance requirements for Sanlam Kenya Plc Group Companies and Sanlam Kenya Plc Associates are provided in the **Sanlam Kenya Plc Governance Policy**.

### 4.2. Risk Management Philosophy

#### Risk management through the ORSA process

The Own Risk and Solvency Assessment (ORSA) is an overarching process that brings together the results from various processes embedded at Sanlam Kenya Plc level as part of the Sanlam Kenya Plc ERM framework. The ORSA process consolidates the various outputs and provides an analysis of the risk capital required to be held in respect of Sanlam Kenya Plc's risks, both currently and over the business planning horizon. The risk and capital assessments in the ORSA take account of Sanlam Kenya Plc's risk profile, approved risk appetite and business strategy.

The Sanlam Kenya Plc risk function, with assistance from the Sanlam Kenya Plc actuarial function, manages the ORSA process and drafts a quarterly Sanlam Kenya Plc ORSA report and Sanlam Kenya Plc Actuarial report, which covers assessments and analysis of Sanlam Kenya Plc's top-down strategic risks, bottom-up operational risks, risk profiles, approved risk appetite, corporate credit risk, liquidity risk, current and projected capital and solvency positions, stress and scenario testing, and projections over the business planning horizon. After management review, the Sanlam Kenya Plc ORSA and Sanlam Kenya Plc Actuarial report is tabled at the Sanlam Kenya Plc Actuarial, Audit, and Risk Committee and Sanlam Kenya Plc Board.

Sanlam is required to submit an annual Sanlam Group (inclusive of Sanlam Kenya Plc as part of the Sanlam Limited Insurance Group) supervisory ORSA report in accordance with the requirements under the Prudential Standards. The Sanlam ORSA process is well established and supported by parallel ORSA processes at Sanlam Kenya Plc level.

Sanlam Kenya Plc adopted the three lines of defence principles for managing risks. These principles define the roles, responsibilities, and accountabilities for managing, reporting, and escalating risks and other matters throughout Sanlam Kenya Plc. The principles incorporate the oversight, management, and assurance of risk management, essentially giving three independent views of risk. This approach ensures that risk management is embedded in the culture and daily activities of Sanlam Kenya Plc Group companies and provides assurance to the Sanlam Kenya Plc Board and Sanlam Kenya Plc Executive committee that risks are managed effectively.

**Sanlam Kenya Plc's businesses are individually responsible for the management of risks in their respective businesses** (i.e., risk identification, analysis, evaluation, and implementation of appropriate risk management actions).

- 4.2.1 The accountability regarding the management of risk rests with the businesses – even if the approach to managing a particular risk has been approved by Sanlam Kenya Plc.
- 4.2.2 For risks with a significant impact, the business must demonstrate that:
  - a) The risk is monitored by the business' operations, as well as independently by the business' risk management function, and
  - b) The business has a clearly defined and documented Risk Appetite.

The above points must be regularly reported to the risk/audit committees/forums.

- 4.2.3 The Sanlam Kenya Plc Head of Risk and Compliance is responsible for monitoring Sanlam Kenya Plc risks on a macro level. Sanlam Kenya Plc risks in this regard refer to the following:
  - a) Risks with a significant financial impact on Sanlam Kenya Plc.
  - b) Risks with a negative reputational impact on Sanlam Kenya Plc.
  - c) Risks that can, owing to their scope, impact negatively on Sanlam Kenya Plc.
  - d) Risks, which within individual businesses, would not fall into any of the above categories but do so when aggregated at Sanlam Kenya Plc level.

The escalation of particular risks to Sanlam Kenya Plc level and the monitoring thereof will be done in accordance with the **Sanlam Kenya Plc Risk Escalation Policy**.

- 4.2.4 The Sanlam Kenya Plc Head of Risk and Compliance has the responsibility to consider decisions, actions or intended actions and risks, brought to his/her attention either by the business heads or other sources, and if he/she concludes that these are or could be detrimental to Sanlam Kenya Plc, it is also his/her responsibility to escalate said actions to the Sanlam Kenya Plc Exco or, alternatively, to insist on measures to reduce or restrict the detrimental effect.
- 4.2.5 Businesses may appeal to the Sanlam Kenya Plc Board if, in their judgement, the Sanlam Kenya Plc Head of Risk and Compliance handling of a function, or a specific decision from him/her, is having or could have a detrimental effect on the functioning of their businesses and on reaching business objectives (e.g., profit targets).
- 4.2.6 The Sanlam Kenya Plc Head of Risk and Compliance will, on an ongoing basis, give the Sanlam Kenya Plc Exco and the Sanlam Kenya Plc Risk and Audit, feedback on risk management in Sanlam Kenya Plc to allow them to fulfil their responsibilities.

- 4.2.7 Each business should determine and document their **risk appetite and tolerance/limit framework** for their operations relative to their budgeted operating profits, Return on Group Equity Value, and Value of New Business, as appropriate.
- 4.2.8 Each business should manage its operations in such a way that the required capital (as prescribed and agreed by the business and Sanlam Kenya Plc) should continuously be covered by the available capital.
- 4.2.9 In general, risks with a small chance of occurring, but with catastrophic results when they occur, should be avoided as far as possible.
- 4.2.10 Each business must be satisfied that the risk-reward profile of any business risk accepted supports its business objective.
- 4.2.11 Each business must determine and document their risk appetite and tolerance/limit framework in respect of reputational and operational risks, including legal and compliance risks aligned with Sanlam Kenya Plc's risk appetite statements and guidance.
- 4.2.12 In general, quantifiable risks (market, credit, life, non-life, etc.) will be measured in terms of the Solvency Capital Requirement (SCR) (or similar measures based on 99.5% confidence interval stresses applied to a market consistent balance sheet over a 1-year time horizon), where such calculations are available. In the absence of Solvency Assessment Management calculations or as appropriate, additional supplementary measures should be used for specific risk categories, for example, sensitivity to local solvency capital requirements, sensitivity of Return on GEV / Value of new business to deviations in best estimate assumptions for underwriting and financial risks.

### 4.3. Risk Management Process

**Each business should have a documented risk management process** that links (i.e., is embedded) into the business's normal management process, and which should cover the following:

- 4.3.1 Establish the risk management context.  
The business should articulate its objectives and define the external and internal parameters to be considered when managing risk, and thus setting the scope and risk criteria for the rest of the risk management process.
  - a) External context (i.e., external environment in which the business seeks to achieve its objectives):  
Define the relationship between the business and its environment, identifying the business's strengths, weaknesses, opportunities, and threats. Determine the crucial elements that may support or impair its ability to manage the risks it faces. Evaluate the key drivers and trends that may impact the objectives of the organisation as well as the perceptions and values of external stakeholders.
  - b) Internal context (i.e., internal environment in which the business seeks to achieve its objectives):  
Understand the business and its capabilities, as well as its goals, objectives, strategies, organisational structure, culture, and values that are in place to achieve them. Risk management's objective is to aid the achievement of the business's goals. As such, the risk management function should facilitate the management of risks by the business.
  - c) Risk management context  
The objectives, strategies, scope and parameters of the business activities or those parts of the business where the risk management process is being applied, should be established. The risk management approach adopted should be

appropriate to the circumstances, to the business and to the risks affecting the achievement of its objectives.

- d) Defining the risk criteria (i.e., setting the risk appetite)  
Decide on the business risk appetite and the criteria against which risk is to be evaluated, to decide on risk acceptability, risk avoidance or risk mitigation.

#### 4.3.2 Risk identification

Define a logical framework for risk identification that ensures that significant risks are not overlooked. Each business needs to put in place demonstrable processes and procedures to ensure that risks are timeously identified. They should also institute methodologies to access possible future risk (i.e., emerging risks) and to increase the probability to anticipate unpredictable risks.

#### 4.3.3 Risk analysis

The risk analysis should separate the minor (acceptable) risks from the major risks and provide data to assist in the evaluation and treatment of risks. It involves the consideration of the sources of risk, their consequences, and the likelihood that these consequences occur. Risk is analysed by combining estimates of consequences (impact) and likelihood of occurrence in the context of existing control measures. It is recommended that significant risks be assessed / re-assessed at least on an annual basis.

The identified key risks that could affect shareholder and relevant stakeholder interests, should be documented together with qualitative or quantitative measures of their likelihood and/or expected impact.

#### 4.3.4 Risk evaluation

The level of risk found during the analysis process needs to be compared with previously established risk criteria (i.e., risk appetite) of the business. This will result in a prioritised list of risks for further action (cost benefit analysis should be deployed to determine whether risk treatment is worthwhile).

Low and accepted risks should be monitored and periodically reviewed to ensure they remain acceptable. Risks above the acceptable threshold will require active management.

#### 4.3.5 Risk treatment

This involves identifying the range of options for treating risk, assessing those options (i.e., cyclical process of deciding whether residual risk levels are tolerable; if not tolerable, considering an alternative risk treatment), preparing risk treatment plans and implementing them.

Risks could be accepted, avoided, transferred (e.g. by re-insurance), prevented or mitigated/minimised. Risks prioritised for further action during risk evaluation should be managed in such a way that the residual risk levels are within the acceptable threshold. The actions required to effectively manage each risk and the method of controlling these actions, should be documented.

The residual risk should be documented and subjected to monitoring, review and, where appropriate, further treatment.

#### 4.3.6 Risk management communication and consultation

The quarterly Sanlam Kenya Plc ORSA process drives the main processes around risk management consultation and communication.

Measures must be in place to ensure:

- a) Communication of the **risk management process** to all who have roles and responsibilities in it to ensure they understand why certain actions are required.

- b) Ongoing communication **and consultation** between all those involved with the process, as well as with stakeholders who are affected by it; and
- c) The documentation of the above.

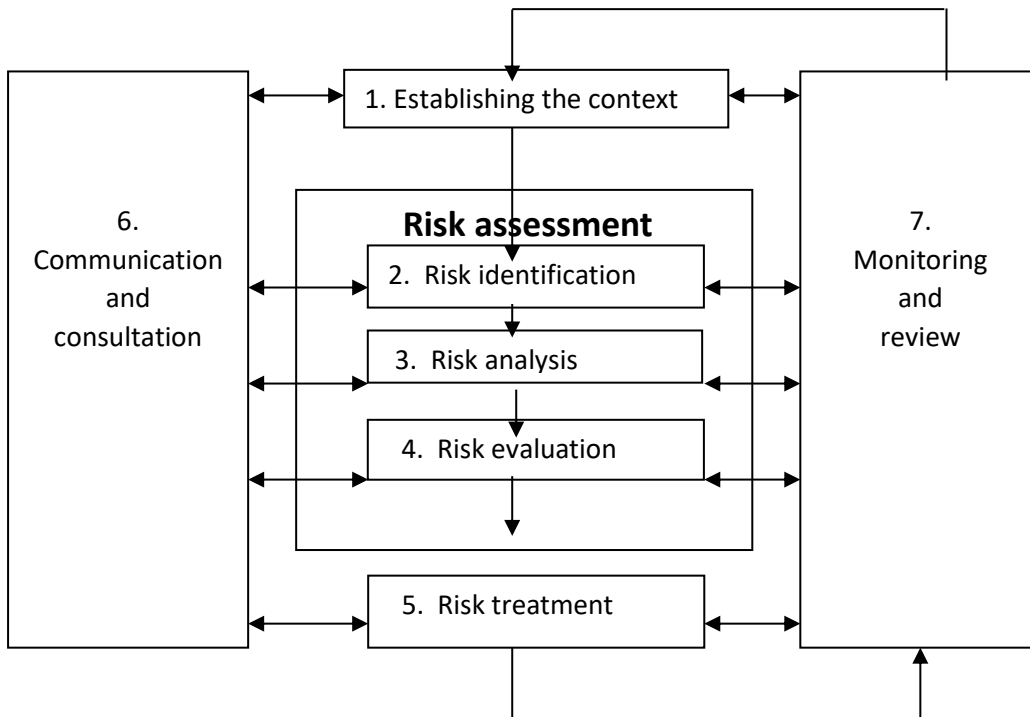
4.3.7 Risk management monitoring and review

Ongoing monitoring and review are essential to ensure that the risk treatment plan remains relevant. The key risk drivers may change, as may the factors which affect the suitability or cost of the various treatment options. It is therefore important to regularly repeat the risk management cycle and review should be an integral part of the risk management treatment plan.

The risk management process should be formally reviewed on a regular basis (at least annually), to determine its effectiveness. The risk management process should be amended as necessary, to ensure the changing needs and circumstances of the business are considered.

Each business risk management process must accordingly be an iterative one, aimed at continuous improvement, which deals not only with existing risks, but can identify new risks and/or opportunities as they emerge. **No risk should be accepted unless it is understood and can be effectively managed.**

Diagram of risk management process

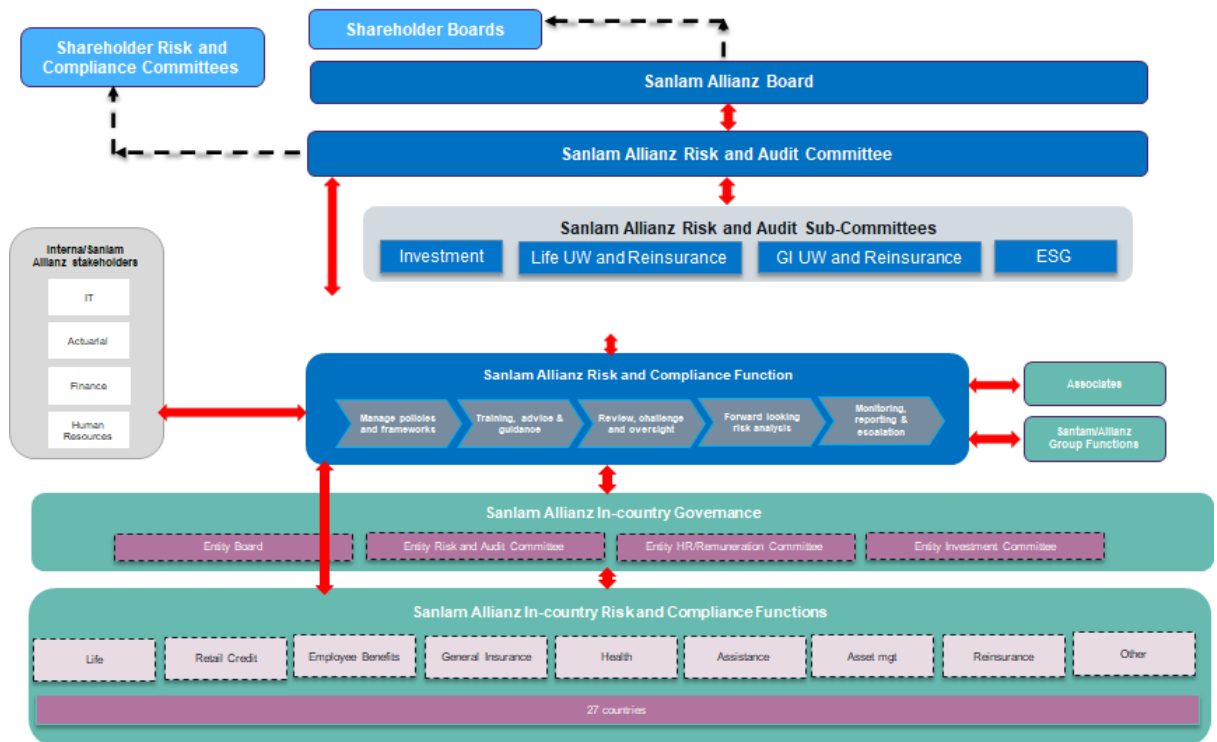


5. Roles and responsibilities for the management of risks

Successful implementation of an Enterprise Risk Management approach to risk management for Sanlam Kenya Plc (at individual business and Sanlam Kenya Plc level) will depend on the contributions of many role players. Each business' risk management policy should set out their respective roles and responsibilities.

The below diagram represents the high-level flow of the risk management function.





The key players and their roles in Sanlam Kenya Plc are:

## 5.1 Sanlam Kenya Plc Board of Directors (the Board)

- 5.1.1 The Board is responsible for the total process of risk management, as well as forming an opinion on the effectiveness of the process.
- 5.1.2 The Board should ensure that a risk management policy is set in conjunction with the executive directors and senior management.
- 5.1.3 The Board should determine the risk appetite and levels of risk tolerance.
- 5.1.4 The Board should delegate to management the responsibility to design, implement and monitor the risk management plan.
- 5.1.5 The Board should ensure that frameworks and methodologies are implemented to increase the probability of anticipating unpredictable risks.
- 5.1.6 The Board is responsible for ensuring that a formal assessment of the risk management processes and outcomes surrounding key risks is undertaken, at least annually, for the purposes of making its public statement on risk management. It should, at appropriately considered intervals, receive and review reports on the risk management process in the company. This risk assessment should address all identified risks.
- 5.1.7 The Board should ensure that there are processes in place enabling complete, timely, relevant, accurate, and accessible risk disclosures to stakeholders.

## 5.2 Sanlam Kenya Plc Actuarial, Audit and Risk Committee

The Sanlam Kenya Plc Risk and Audit Committee will assist the Sanlam Kenya Plc Board in fulfilling its risk responsibilities, that is, inter alia reviewing the risk management process and significant risks facing Sanlam Kenya Plc or the relevant businesses in Sanlam Kenya Plc. The results of this work must be reported to and considered by the Sanlam Kenya Plc Board.

### **5.3 Other governance committees/forums**

The following sub-committees/forums will assist the Sanlam Kenya Plc Risk and Audit Committee in fulfilling its risk responsibilities that is, inter alia reviewing the risk management process and significant risks facing Sanlam Kenya Plc or the relevant business. These (more detail on these committees/forums in the Sanlam Kenya Plc ERM Framework) include:

- 5.3.1 Sanlam Kenya Plc Investment committee
- 5.3.2 Human Resources, Nomination and Remuneration Committee

### **5.4 Chief Executive Officer (of Sanlam Kenya Plc, as well as, of each business)**

- 5.4.1 The Chief Executive Officer (“CEO”) brings the power of his/her office to ensure the implementation of risk architecture operationally.
- 5.4.2 The CEO must support, and be clearly and actively supporting, the necessary focus on risk management.

### **5.5 Sanlam Kenya Plc Executive Committee (Exco)**

The Executive Committee must ensure that the business achieves its strategic goals in a manner that optimises its risk-adjusted return performance. In particular, it has the executive responsibilities relating to the Board’s oversight responsibilities. This includes:

- 5.5.1 Accountability to the Sanlam Kenya Plc Board for designing, implementing, and monitoring the process of risk management and integrating it into the day-to-day activities of the company.
- 5.5.2 Providing the Sanlam Kenya Plc Board with assurance that the above has been done, and the way this has been done).
- 5.5.3 Ensuring that generally accepted risk management frameworks and models, including internal controls, are embedded in organisational operations and processes.
- 5.5.4 Clearly communicating the risk management policy to all employees to ensure that risk awareness is embedded into the language and culture of the business.
- 5.5.5 The risk management process relates to all risks in the business’ sphere of responsibility, irrespective of geographical location.

### **5.6 Sanlam Kenya Plc Head of Risk and Compliance**

The overall role of the Sanlam Kenya Plc Risk Management function under the leadership of the Head of Risk and Compliance is to develop, implement, monitor, and continuously improve Sanlam Kenya Plc’s risk management processes, in conjunction with the Sanlam Kenya Plc businesses, to ensure that it functions adequately, consistently, and effectively across Sanlam Kenya Plc.

The Sanlam Kenya Plc Head of Risk and Compliance should perform the following functions:

- 5.6.1 Primarily, assist and guide the risk officers and senior risk officers to implement the risk management framework and working with it on an ongoing basis, ensuring that it is suitably reviewed and regularly updated to address new elements of risk in the business.
- 5.6.2 Ensure that all underlying businesses within Sanlam Kenya Plc are included in the risk management and risk reporting function.

- 5.6.3 Monitoring Sanlam Kenya Plc's entire risk profile, ensuring that major risks are identified, appropriately managed, and reported upwards.
- 5.6.4 Provide and maintain the risk management infrastructure to assist the Sanlam Kenya Plc Board in fulfilling its responsibilities.
- 5.6.5 Assist in the execution of the risk management process, but the accountability to the Sanlam Kenya Plc Board (who is ultimately responsible) remains with the management.
- 5.6.6 Liaison with the Sanlam CRO / Sanlam Risk Management under the requirements of group supervision for the Sanlam Limited Insurance Group.
- 5.6.7 Submit quarterly Sanlam Kenya Plc ORSA updates to the Sanlam Kenya Plc and Sanlam governance structures.

## **5.7 Sanlam Group Risk Forum**

Sanlam Kenya Plc will participate in the Sanlam Group Risk Forum to benefit from the coordination and transfer of knowledge between Sanlam and other businesses in the Sanlam Group, and to assist in identifying common risk management issues, including further alignment/enhancement of the Sanlam Kenya Plc ORSA processes, specific risks to conduct group-wide deep dives and sharing risk insights. It will also provide a platform to discuss emerging risks.

## **5.8 Sanlam Kenya Plc Group company Boards**

Sanlam Kenya Plc Group company Boards are responsible for the total risk management process in the respective companies.

## **5.9 Sanlam Kenya Plc Group company Committees**

Assist the Sanlam Kenya Plc Group company Board in fulfilling its responsibilities to the Sanlam Kenya Plc Board.

## **5.10 Sanlam Kenya Plc Group company committees**

Depending on the size, complexity and nature of risks encountered in each company, other executive level management committees may be created to assist their Executive Committees in fulfilling its responsibilities. Should this be the case, their roles and responsibilities should be covered in the risk management framework of the company concerned.

## **5.11 Risk management functions in each Sanlam Kenya Plc Group company**

Every Sanlam Kenya Plc Group company must:

- 5.11.1 Establish a risk management function. In respect of every compliance function established in terms of this Policy:
  - a. ensure the independence of the function (direct reporting line to the entity CEO is required and exceptions should be approved by the SanlamAllianz (CRO).
  - b. ensure that the function is adequately resourced in terms of human-, financial- and technological resources.
  - c. appoint a person with sufficient status, skills, and knowledge to act as the head of the function.
  - d. ensure a dotted reporting line of the Head of the function to the Sanlam Kenya Plc Head of Risk and Compliance.

- e. ensure that the job description of the Head of the function is approved by the Sanlam Kenya Plc Head of Risk and Compliance
- f. Ensure that the target setting and the annual assessment for the Head of Risk is signed off by the Sanlam Kenya Plc Head of Risk and Compliance. Any nomination or dismissal of a Head of Risk requires the written pre-approval of the Sanlam Kenya Plc Head of Risk and Compliance, that includes the assessment of qualification, e.g. based on CV and interviews.
- g. Sufficient budget should be provided to the function to finance regular and annual tasks.

The Head of Risk function for each company should perform the following functions:

- 5.11.2 Primarily, assist and guide the line managers to implement the risk management framework and working with it on an ongoing basis, ensuring that it is suitably reviewed and regularly updated to address new elements of risk in the company.
- 5.11.3 Monitoring the company's entire risk profile, ensuring that major risks are identified, appropriately managed, and reported upwards (using the Risk Reporting Template as shown in Appendix A).
- 5.11.4 Provide and maintain the risk management infrastructure to assist the company Board in fulfilling its responsibilities.
- 5.11.5 Assist in the execution of the risk management process, but the accountability to the company Board (who is ultimately responsible) remains with the management.
- 5.11.6 Escalate risks to Sanlam Kenya Plc level in accordance with Sanlam Kenya Plc Risk Escalation Policy (using the Risk Reporting Template as shown in Appendix A).
- 5.11.7 Liaise with the Sanlam Kenya Plc Head of Risk and Compliance.

## **5.12 Line manager in each Sanlam Kenya Plc Group company**

Line managers should:

- 5.12.1 Identify and evaluate the risks faced by their company for consideration by their company Boards.
- 5.12.2 Design, operate and monitor a system of internal control appropriate for the needs of their company.
- 5.12.3 Embed control and compliance responsibilities within employees' job descriptions and performance objectives.
- 5.12.4 Implement all relevant Sanlam Kenya Plc policies.
- 5.12.5 Escalate risks to the company Head of Risk and Compliance in accordance with the company's Risk Escalation Policy.

## **5.13 Sanlam Kenya Plc Operations and IT Function**

IT risks are managed across Sanlam Kenya Plc in an integrated manner following the Sanlam Kenya Plc ERM Framework. Sanlam Kenya Plc's Operations and IT function is the custodian of Sanlam Kenya Plc's IT Policy framework and ensures explicit focus on, and integration, with the Sanlam IT Governance framework, which includes the governance of Information Security.

The Sanlam Kenya Plc Head of ICT facilitates the process of identifying emerging IT risks, as well as unpacking significant IT risks with Sanlam Kenya Plc -wide strategic or

operational impact. The Sanlam Kenya Plc Actuarial, Audit, and Risk committee provides guidance to the Head of ICT in terms of appropriate response, such as the establishment of policy.

A quarterly IT Governance report, summarising the Sanlam Kenya Plc -wide situation is delivered to the Sanlam Kenya Plc Actuarial, Audit, and Risk committee.

#### **5.14 Internal Audit**

The internal audit function is performed by Sanlam Group Head of Internal Audit.

Internal Audit does not assume responsibility for the functions, systems, and process of risk management, but rather it assists the Sanlam Kenya Plc Board and management in the monitoring of risk management in Sanlam Kenya Plc.

Sanlam Internal Audit, in conjunction with the Sanlam Kenya Plc Head of Risk and Compliance and Sanlam Kenya Plc Group company Heads of Risk/Risk officers, monitors, through its own assurance processes, the progress of companies in managing their risks.

Sanlam Internal Audit assumes responsibility for providing independent assurance on the adequacy and effectiveness of the risk management process. Where an external independent assurance provider is utilised, Sanlam Internal Audit will also facilitate the engagement.

#### **5.15 Forensics**

Sanlam Kenya Plc has a Forensics department which carries out forensics' investigations.

#### **5.15 Sanlam Kenya Plc Chief Financial Officer (CFO)/Financial Manager**

Sanlam Kenya Plc does not have a CFO/Finance Manager. However, Sanlam General Insurance and Sanlam Life Insurance have Heads of Finance. The Heads of Finance in SGIL and SLIL are responsible to ensure that sound financial practices are followed, adequate and accurate reporting occurs, and financial mis-statement risk is minimised.

#### **5.17 Sanlam Kenya Plc Exco Functions**

The respective Sanlam Kenya Plc Exco members responsible for Operations and IT, HR, Actuarial, Finance and Brand (including Marketing, Corporate Affairs, and Communications) will be responsible for the risk management process in these areas.

#### **5.18 Sanlam Kenya Plc Actuarial**

The measurement of the sensitivity of the financial position of the insurance operations to deviation from expectations of future experience will form part of the regular actuarial investigations and reports. Although it is a separate reporting function, inputs on key risks will be made into risk management.

### **6. Monitoring compliance with the policy**

#### **6.1. Formal Self-Assessments**

Each business unit / entity is required to perform a risk management maturity self-assessment on a regular basis. Sanlam Kenya Plc is responsible for summarising these results and presenting the results at the Sanlam Kenya Plc Actuarial, Audit and Risk committee.

The risk management maturity self-assessment should be conducted according to the self-assessment methodology prescribed by Sanlam.

Each business should review and report on its risk management process, the aim of such reviews being to improve the process, and to modify it in the light of changed circumstances. The focus of the reviews, and the contents of the reports, should be on issues such as:

- 6.1.1 The existence, completeness, and effectiveness of the risk management process.
- 6.1.2 The suitability of the climate within which risk management takes place (e.g., is there adequate top-level support, is there a suitable risk culture, are there sufficient capable resources, etc.).
- 6.1.3 Whether the risk profiles and risk reporting adequately communicate the business's risks to senior levels, in a way that contributes to improved decision-making.

Areas for improvement in maturity and related actions plans must be incorporated into the risk management plans for the next year.

## **6.2 Independent Assurance**

Sanlam Internal Audit should perform independent assurance over the risk management functions of business units on a rotational basis. The results should be formally reported back to the Sanlam Kenya Plc Actuarial, Audit and Risk committee as well as Sanlam.

## **6.3 Management Representations**

Businesses are also required to provide assurance over the risk management process and framework in place within the business on an annual basis through management representations.

## **6.4 Annual Risk Plans**

Sanlam Kenya Plc must submit its risk plan for the year to Sanlam Group and each business within Sanlam Kenya Plc must submit their risk plans for the year to the Sanlam Kenya Plc Risk Management function.

# **7. Reporting on policy outcomes**

## **7.1. Monitoring and reporting of risks**

Each business should develop and continuously update profiles of risks it is exposed to, according to its own business needs and requirements. The Sanlam Kenya Plc risk profile will consist of an aggregation of the risk profiles of the businesses, combined with the effect of risks that exist at the Sanlam Kenya Plc level only. It is therefore necessary to have minimum levels of consistency and standardization in the development of risk profiles (and reporting thereon).

- 7.1.1 Each business should regularly monitor its risks, and report on them to the relevant Excos, Boards and Risk and/or Audit Committees a copy of which should be provided to Sanlam Kenya Plc. The contents and frequency of these risk reports will depend on the nature, scale, priority, and complexity of the risks involved. The risk reports should include qualitative comments on the risks reported on (e.g., nature of contentious issues, recent breaches of important limits or procedures, and material breakdowns in controls) and where appropriate, quantitative measures should also be given.
- 7.1.2 Sanlam Kenya Plc is required to prepare a quarterly Sanlam Kenya Plc ORSA update which will cover top-down strategic risks as well as the bottom-up operational risks within Sanlam Kenya Plc. The ORSA update must also include appetite statements, emerging risks, capital and solvency requirements, stress and scenario testing and business projections under base case and adverse scenarios. The Sanlam Kenya Plc ORSA will be presented at the Sanlam Kenya Plc Exco and Sanlam Kenya Plc Risk and Audit committee.

- 7.1.3 Sanlam Kenya Plc will also provide the Sanlam Kenya Plc ORSA to Sanlam Group to enable Sanlam reporting as required under group supervision for the Sanlam Limited Insurance Group of which Sanlam Kenya Plc forms a part.
- 7.1.4 At Sanlam Kenya Plc level the following Risks will be reported on at the Sanlam Kenya Plc Exco, and Sanlam Kenya Plc Actuarial, Audit and Risk committee meetings:
- a) Risks with a significant financial impact on Sanlam Kenya Plc.
  - b) Risks with a negative reputational impact on Sanlam Kenya Plc
  - c) Risks that can, owing to their scope, impact negatively on Sanlam Kenya Plc.
  - d) Risks, which within individual businesses, would not fall into any of the above categories, but do so when accumulated at Sanlam Kenya Plc level.
- 7.1.5 Risks requiring escalation will be reported and managed in accordance with the Sanlam Kenya Plc Risk Escalation Policy.
- 7.1.6 Key Risk indicators (KRIs) of a business must be identified and monitored as part of a regular review of processes and procedures to ensure the effectiveness of its internal systems of control, so that its decision-making capability and the accuracy of its reporting and financial results are maintained at a high level at all times.

## 7.2. Disclosures in relation to risk management

The Sanlam Kenya Plc Board or applicable governance body (of each business and Sanlam Kenya Plc) is responsible for **mandatory disclosures** in relation to risk management of its business, including disclosures required in the integrated annual report. It should as a minimum disclose:


- 7.2.1 That it is accountable for the process of risk management and the system of internal control, which is regularly reviewed for effectiveness.
- 7.2.2 That there is an ongoing process for identifying, analysing, evaluating and managing the significant risks faced by the company, which has been in place for the year under review as well as for the period between the relevant year end and the date of approval of the annual report and accounts.
- 7.2.3 That there is an adequate and effective system of internal control in place to mitigate the significant risks faced by the company to an acceptable level. Such system is designed to manage, rather than eliminate, the risk of failure or maximising opportunities to achieve business objectives and can only provide reasonable but not absolute assurance.
- 7.2.4 That there is a documented and tested process in place, which will allow the company to continue its critical business processes in the event of a disastrous incident impacting its activities. This is commonly known as a business continuity plan and should cater for a worst-case scenario.
- 7.2.5 The Board or governance body's view on the effectiveness of the risk management process.
- 7.2.6 Any undue, unexpected, or unusual risks.

Where the Board or governance body cannot make any of the disclosures set out above, it should state this fact and provide a suitable explanation.

**Sanlam Kenya Plc Risk Reporting Template**

**<<Insert Entity Name>>: KEY RISK REPORT/RISK ESCALATION REPORT**

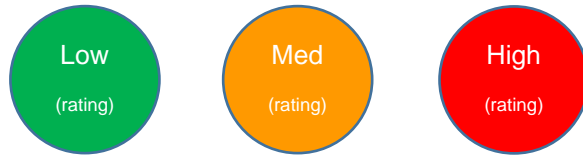
Top risks for [the quarter ended] <<Insert Date>>

Risk	Risk Discussion														
<p><b>1.&lt;&lt; Insert highest rated risk – risk 1&gt;&gt;</b></p> <div style="text-align: center;">  <p>High (rating)</p> </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th colspan="2" style="background-color: #cccccc;">Relative Ranking</th> </tr> <tr> <td style="width: 50%; text-align: center;">&lt;&lt;Previous Quarter&gt;&gt;</td> <td style="width: 50%; text-align: center;">&lt;&lt;Ranking&gt;&gt;</td> </tr> <tr> <td style="text-align: center;">&lt;&lt;Current Quarter&gt;&gt;</td> <td style="text-align: center;">&lt;&lt;Ranking&gt;&gt;</td> </tr> <tr> <th colspan="2" style="background-color: #cccccc;">Trend in Risk Exposure</th> </tr> <tr> <td style="text-align: center;">&lt;&lt;Previous Quarter&gt;&gt;</td> <td style="text-align: center;">&lt;&lt;Trend indicator&gt;&gt;</td> </tr> <tr> <td style="text-align: center;">&lt;&lt;Current Quarter&gt;&gt;</td> <td style="text-align: center;">&lt;&lt;Trend indicator&gt;&gt;</td> </tr> <tr> <td colspan="2" style="background-color: #cccccc;">Owner: &lt;&lt;Name of risk owner&gt;&gt;</td> </tr> </table>	Relative Ranking		<<Previous Quarter>>	<<Ranking>>	<<Current Quarter>>	<<Ranking>>	Trend in Risk Exposure		<<Previous Quarter>>	<<Trend indicator>>	<<Current Quarter>>	<<Trend indicator>>	Owner: <<Name of risk owner>>		<p><b>Risk Description:</b> &lt;&lt; Provide a brief description of the risk&gt;&gt;</p> <p><b>Risk Impact:</b> &lt;&lt;Provide information on the risk impact of this risk on the business&gt;&gt;</p> <p><b>Mitigation Actions:</b> &lt;&lt;Provide information on the actions taken to mitigate the risk&gt;&gt;</p> <p><b>Target Date:</b> &lt;&lt;Provide target date for the mitigating actions&gt;&gt;</p>
Relative Ranking															
<<Previous Quarter>>	<<Ranking>>														
<<Current Quarter>>	<<Ranking>>														
Trend in Risk Exposure															
<<Previous Quarter>>	<<Trend indicator>>														
<<Current Quarter>>	<<Trend indicator>>														
Owner: <<Name of risk owner>>															

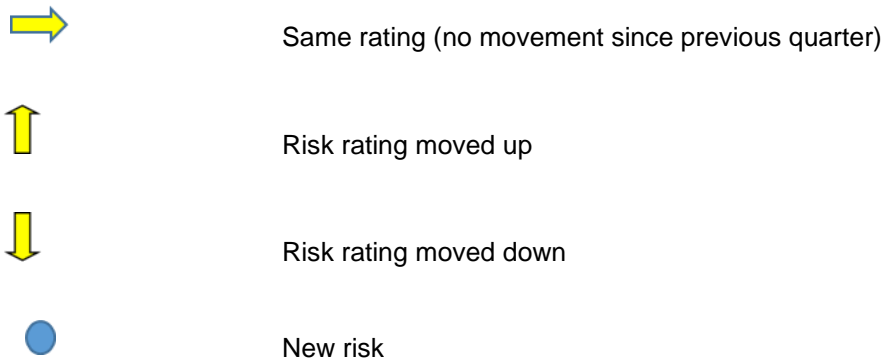
1. Repeat information above per risk for all the top risks
2. Complete the table using the following indicators



- **Insert the rating bubble as per the risk rating calculated:**



- **Provide the ranking:**  
This is the actual ranking (1 – 10) as per previous quarter versus the ranking in this quarter, for example if a risk has moved from the number 1 risk the previous quarter, to the number 4 risk this quarter, it will be indicated as “1” for the previous quarter and “4” for the current quarter.
- **Provide the trend:**  
Did the risk move up, down or not at all from the previous quarter.



### 3. Risk rating methodology that could be used

Impact rating	% of Tolerance Limit (TL)	Effect on Sanlam company's:	
		Annual Operating Profit After Tax and Minorities	Group Equity Value (GEV)

R million			*TL <sub>1</sub> = Rxxxm	**TL <sub>2</sub> = Rxxxm
1	Insignificant	0% to <1%		
2	Minor	1% to <5%		
3	Moderate Minus	5% to <20%		
4	Moderate Plus	20% to <50%		
5	Major	50% to <100%		
6	Extreme	100% plus		

\*TL<sub>1</sub> is the Tolerance Limit expressed in terms of operating profits [10% of annual net profit after tax and minorities of Rxxxm for 2023]

\*\*TL<sub>2</sub> is the Tolerance Limit expressed in terms of Group Equity Value (GEV) [7.5% of GEV of Rxxxm at the start of 2023]

Likelihood rating		Approximate probabilities
1	Rare	0% to <1%
2	Unlikely	1% to <5%
3	Possible Minus	5% to <20%
4	Possible Plus	20% to <50%
5	Likely	50% to <80%
6	Almost certain	80% to <100%

Type of Risk Event			Likelihood						
			1	2	3	4	5	6	
			Rare	Unlikely	Possible Minus	Possible Plus	Likely	Almost Certain	
			0% to <1%	1% to <5%	5% to <20%	20% to <50%	50% to <80%	80% to <100%	
Impact	6	Extreme	100% plus	Medium - 6	Medium - 12	High - 18	Very High - 24	Very High - 30	Very High - 36
	5	Major	50% to <100%	Low - 5	Medium - 10	High - 15	High - 20	Very High - 30	Very High - 30
	4	Moderate Plus	20% to <50%	Low - 4	Medium - 8	Medium - 12	High - 16	High - 20	Very High - 24
	3	Moderate Minus	5% to <20%	Low - 3	Medium - 6	Medium - 9	Medium - 12	High - 15	High - 18
	2	Minor	1% to <5%	Low - 2	Low - 4	Medium - 6	Medium - 8	Medium - 10	Medium - 12
	1	Insignificant	0% to <1%	Low - 1	Low - 2	Low - 3	Low - 4	Low - 5	Medium - 6

Residual Risk Rating	Description
Low	Low risk: manage by routine procedures
Medium	Medium risk: management responsibility must be specified
High	High risk: management attention required
Very High	Very High risk: executive intervention required