RISK MANAGEMENT POLICY

Table of Contents

1. BACKGROUND

The underlying premise of Enterprise Risk Management is that every entity exists to provide value for its stakeholders. All entities face uncertainty and the challenge for management is to determine how much uncertainty to accept, as it strives to grow shareholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value.

Risk Management enables management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value.

This document outlines the Enterprise Risk Management Policy at AfroCentric Group ("the Group"). It is intended to provide guidance on implementing an effective Enterprise Risk Management (ERM) program in the Group.

The Risk Management Policy specifically addresses the structures, processes to be implemented to manage risks on an enterprise-wide basis in a consistent manner. It also addresses the specific responsibilities and accountabilities for risk management within the Group and its subsidiaries.

2. POLICY STATEMENT

The management of the Group is committed to sound enterprise risk management practices. Active risk awareness and optimal management of risk and associated exposures are embedded throughout the business.

The Policy includes the following main components:

- The broad objectives and philosophy of risk management in the Group;
- The roles and responsibilities of the various functionaries in the Group tasked with risk management; and
- Minimum standards for the implementation of risk management in the various business units within the Group.

3. POLICY OBJECTIVES

The objective of Afrocentric's Enterprise Risk Management approach is to support the Group in achieving its primary objective of optimising return on Group equity and to protect and grow shareholder value within the Group's approved Risk Appetite.

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

- Supporting the Group's strategic business goals;
- Safeguarding of the Group's assets (including information) and investments;
- Supporting business sustainability under normal as well as under adverse operating conditions;
- To provide reliable information about risks affecting the achievement of the Group's core objectives; and
- Behaving responsibly towards all stakeholders with a legitimate interest in the Group.

4. SCOPE OF APPLICATION

This policy applies to the entire Group and its subsidiaries. All permanent staff, fixed term contractors, independent contractors and any other individuals conducting work in the Group and at any of its locations and points of representation are required to conform to this policy.

5. RELEVANT LEGISLATION AND GUIDELINES

King IV Principles on Risk Governance: The governing body ("the Board") should govern risk in a way that supports the organisation in setting and achieving its strategic objectives.

Medical Schemes Act, 131 of 1998: Requires that administrators and managed care organisations be accredited as such by the Council for Medical Schemes before they may administer a medical scheme or render managed care services to a medical scheme.

Companies Act 71 0f 2008: has legislated key governance best practices.

6. RELATED POLICIES

This policy should be read in conjunction with the following policies and frameworks:

- Afrocentric Enterprise Risk Management Framework
- Technology and Information Governance Framework
- Business Continuity Management (BCM) Policy
- Compliance Risk Management Policy
- Disciplinary Management Policy
- Fraud Prevention and Management Policy
- Environmental Health and Safety Policy

7. DEFINITION OF TERMS

TERM	DESCRIPTION
Enterprise Risk Management	Enterprise Risk Management (ERM) is a high-level over-arching framework aimed at ensuring that: • All risks which could jeopardise / enhance the achievement of the Group's strategic goals will be identified; • Appropriate structures, policies, procedures, and practices are in place to manage these risks;
Emerging Risks	Emerging risks represent known or unknown risks with a significant potential impact on business, but for which the likely severity for the Group and its businesses have not been assessed or is difficult to quantify (either because the likelihood of such an event occurring is unknown or because the full impact of such an event, should it materialise, is unknown).
Inherent and Residual Risk	The net risk exposure can be quantified either on an inherent or a residual basis: • Inherent risk: the net exposure (likely impact), without any mitigation actions or other controls in place.

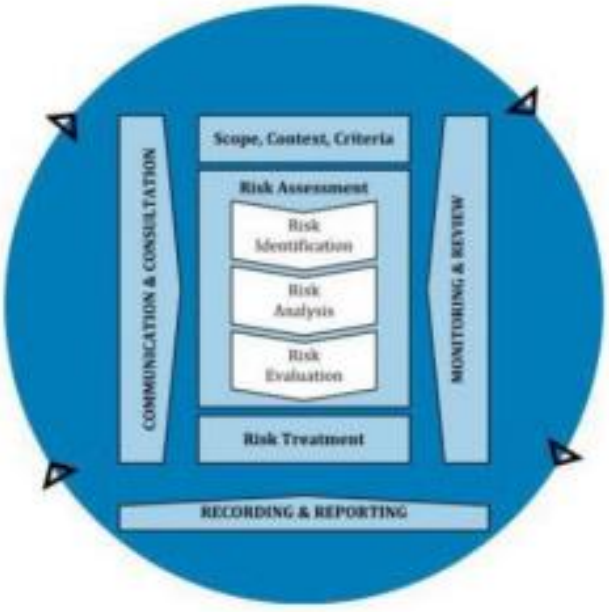
	Residual risk the net exposure, allowing for the effectiveness of the existing controls as well as any additional risk mitigation actions defined.
Risk	Risk is inherent to the business of the group and is defined as the threat that a condition, an event, action or inaction will adversely affect the Group's ability to achieve its business objectives, including strategic, operational, financial and compliance objectives. Business risk arises as much from the possibility that threats will materialise as it does from the possibility that opportunities will not be realised. The Group's Risk Management process is aimed at managing each of the three elements of risks: • Opportunities: upside risks, or the "offensive" perspective of risk (looking for opportunities to exploit). • Hazards: downside risks, or the "defensive" aspect of risk (focusing on prevention or mitigation of the threats and vulnerabilities that could generate losses). • Uncertainties: the volatility aspect of risk (risks to be managed to improve the predictability of outcomes/performance).
Risk Appetite	This is an overall indication of the level and type of risk that an organization is prepared to accept in the pursuit of its goals. The risk appetite can be defined for the Group or for the respective business divisions and subsidiaries within the clusters. The risk appetite statement should remain strategic in nature.
Risk Champions	A Risk Champion is a person who by virtue of his /her expertise or authority, champions a particular aspect of the Risk Management Process. It must be clear that a risk champion is not necessarily a risk owner; however, he/she plays a critical role in supporting the Risk Management Process in specific allocated areas of functions.
Risk Event	The materialising (whether partially or in full) of risk, whether the risk has previously been identified or not. For existing risks, related events can assist in the quantification of the risk.
Risk Function	The Risk Management team serves as base for risk management advisory service for Afrocentric Health.
Risk Management	Is an on-going process, involving the Board of Directors, management and other personnel. It is a systematic approach to setting the best course of action to manage uncertainty by identifying, analysing, assessing, responding to, monitoring and communicating risk issues/events that may have an impact on an organization successfully achieving their business objectives.

Risk Management System	BarnOwl and CURA
Risk Tolerance levels	This is the more tactical interpretation of the strategic risk appetite and provides business with certain boundaries/ranges for different risk types. It can be defined either: • Qualitatively: on a relative scale (e.g., high, moderate or low) or • Quantitatively: in terms of a quantifiable metric, (e.g., as a risk-adjusted shareholder value such as Return on Group Equity Value, Return on Embedded Value, or Risk Adjusted Performance Measurement.)

8. RISK MANAGEMENT PROCESS

The Group 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. The process will cover the planning, arranging, and controlling of activities and resources to minimise the potential likelihood and impact of risks to levels within the risk appetite. Although the risk management process is considered a separate management discipline, it should be integrated and aligned with the regular management processes.

The Risk Management System must be used for the recording and monitoring of all operational business risks and significant events of the risk materialising. The risk management process is iterative and can be summarised as follows:



8.1. Establishing Context

The first step in the Risk Management value chain is establishing the context, which includes taking the external and internal environment which the Group is exposed to into consideration to achieve its goals.

For the risk management processes to be effective, it is important that the Executive Enterprise Risk Committee (EERCO) and Audit and Risk Committee (ARC), management and individuals assigned with risk management responsibilities (Risk Champions) clearly understand:

- The relationship between the business and its operating environment.
- The business's strengths, weaknesses, opportunities and threats.
- The crucial elements that might support or impair its ability to manage the risks it faces.
- The business capabilities and its goals, objectives, strategies and values and the drivers of these.
- The financial planning cycle of the business.

The understanding and on-going monitoring of these aspects will assist in the pro-active identification of existing and emerging risks. The Chief Risk Officer should maintain risk evaluation criteria and a logical, practical framework for the identification and analysis of risk and its root causes. The Chief Risk Officer should also assist the various businesses to set the goals, objectives and boundaries of the risk management processes appropriate for their respective environments.

8.2. Risk Identification

During this qualitative step, the following should be determined:

- What is the risk? (clear definition, highlighting the impact that the risk posed to the business).
- What is the type and category of the risk?
- What are the root causes of the risk? (what will determine whether the risk will materialise or the severity of the impact)?
- What are the potential consequences, should the risk materialise?
- Which objectives of the business may be impacted by the risk?

Various techniques may be used by the respective levels of management to identify risk. Examples include risk assessment workshops, strategy sessions, analysis of key incidents, key risk indicators, monitoring of controls in operations, analysis of key business drivers, analysis of key processes and analysis of root causes of major external risk events.

Risk Specialists should work closely with the other assurance providers (e.g., Internal and External Audit, Compliance, Legal and Forensic Services) to ensure that all significant risks are identified (either individually or cumulatively). Regular assessments of emerging risks (at least annually) must be conducted to ensure that all relevant risks are included in the Group's risk profile. To this end, the Chief Risk Officer must ensure that global studies of emerging risks are analysed and the potential impact on the Group's goals are reviewed with the risk owners, to determine whether new risks should be included in the Group's strategic risk register.

8.3. Risk Analysis and Evaluation

The risk analysis should separate the minor (acceptable) risks from the more significant 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.

This quantitative step includes an analysis and assessment of:

- The inherent financial impact should the risk materialise: This assessment is done on the basis that all existing controls and mitigation actions will fail, or the controls to mitigate the risk are not available. The time horizon of the quantification of risks is normally (at least) one year in the future (forward-looking).
- The residual financial impact if the risk materialises within the next year: This is done on a residual basis, assessing the residual likelihood and residual impact, i.e., assuming that the existing controls and additional mitigating actions, realistically being implemented, will be effective. Pre-determined rating scales (Refer to Annexure A) must be applied, but actual monetary values within the identified impact range may be specified where deemed more appropriate.
- It is not always that simple to quantify the likely impact (e.g., for reputational risks), but Impact matrixes can be used, where different levels of consequence are aligned with the different impact scales (e.g., for reputational risk different levels of exposure or media coverage can be used to indicate the likely impact). It is important to quantify the residual impact as closely as possible, to maintain the integrity of the aggregate holistic view of the risks of the Group.
- The Risk Management System will assist in the calculation of the residual combined rating. This can be expressed as a monetary amount (impact x likelihood) and will be used to determine exposure to significant risks (in order to optimise resources).
- Determine the Risk Control Effectiveness: This assessment indicates the level of effectiveness of existing risk management activities.
- Identify related controls: In order to assist Internal Audit in their risk-based audit approach, the significant controls impacting the risk (mitigation) should be identified and linked to the risk. A standard classification of controls was defined and deployed on the Risk Management System.

The assessed level of residual risk, compared with the risk appetite and tolerance levels of the Group, will determine the prioritised list of key risks for further detailed action and monitoring. Risks currently rated as Low or Medium must still be reviewed regularly to ensure that the levels of threat remain acceptable.

Particular attention must be given to risk with a low likelihood, but extremely high impact, to ensure that controls managing the likelihood remain effective.

8.4. 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 and mitigated (prevented /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 plans.

8.5. Ongoing Monitoring and Reporting

8.5.1. Monitoring

Residual risk profiles must be reviewed regularly to determine the effectiveness and progress with management actions.

8.5.2. Key Risk Indicators

Each business unit and subsidiary is responsible for defining, monitoring and reporting on Key Risk Indicators for all key risks identified.

8.5.3. Reporting

Each business should develop and continuously update profiles of the risks it is exposed to, according to its own business needs and requirements.

Basic protocols include:

- Quarterly reporting of significant risks and progress with action plans via the Business Unit/Divisional Enterprise Risk Committees and Executive Enterprise Risk Committee to ensure accurate reporting to the Audit and Risk Committee.
- Monthly reporting of significant new risks, incidents and near miss events or progress on existing risk events.
- Escalation of risks to appropriate levels of oversight and with appropriate urgency as per the Escalation Framework

The risk reporting and consolidation process can be depicted as follows:

9. RISK APPETITE

The Audit and Risk Committee reviews the appropriateness of the Group's Risk Management Policy, including Risk Appetite Statements, i.e., the maximum acceptable level of risk that the Group may undertake. In order to monitor adherence to this overall strategic appetite, relevant supporting Risk Tolerance levels are defined and monitored on a regular basis. Material operating entities within the Group must define similar more granular tolerance levels (appropriate for their level of operations) subject to the approval thereof by Audit and Risk Committee.)

The responsibility for the management of risk in the Group vests with the business units/management ("first line of defence"), even if the approach to managing a particular risk has been approved by the Chief Risk Officer.

The businesses are assisted by the ERM structures (such as the Risk and Compliance Division and Head(s) of Risk Management Control – "second line of defence") and supported by the risk management culture set by the Executive Committee (Exco).

ERM within the Group is further strengthened by (internal) audit ("third line of defence") that will assess the adequacy and the effectiveness of the risk management processes regularly, and report to the Audit and Risk Committee on the assessment. This is in line with the Sanlam Board's adoption of the three lines of defence model for managing risks. The model is depicted below.

The Chief Risk Officer determines the relevant risk management framework for the Group in accordance with the Group guidelines and policies. The Chief Risk Officer monitors the risk management process and profile of the Group at an enterprise level and as such will rely on various specialist risk management functions (such as Compliance).

The escalation of risks to the attention of the ARC must be done in accordance with the Risk Escalation Matrix which is aligned with the Group escalation requirements. Depending on the level of classification of a risk, the Chief Risk Officer has the responsibility to consider risk management related decisions, risk mitigation actions and risks taken by the Group, and the responsibility to approve (and where appropriate) require additional measures to reduce or restrict the potential negative effect of exposures the Group.

Where the required consensus with business is not reached, this must be reported to the Sanlam Ltd Exco & Board. SLS business may appeal such an intervention to the Sanlam Ltd Exco.

10.SIGNIFICANT RISK CATEGORIES

The identification of risks and the reporting there-on are directed by the Risk Categories standard, which may be adjusted from time to time to accommodate the reporting requirements of the Sanlam Group.

The major risk categories for the Group are:

- Strategic Risk.
- Market Risk.
- Funding Liquidity Risk.
- Operational Risk.
- Conduct Risk.
- Brand and Reputational Risk.

11.RISK EVENT RECORDING

The risk event (incident) management process follows a similar iterative process as the risk management process. An important component of risk event recording and management is to link a particular event/incident to the underlying risk and relevant risk category to enhance the quantification of risks within the respective categories. The Risk Management System provides for the recording and monitoring of risk events.

11.1. Risk Event Register

All entities within the Group should ensure that relevant quantitative data on incidents and losses is properly recorded and readily available for internal analysis as well as regulatory reporting requirements.

11.2. Purpose

A risk event denotes any operational risk incident or experience that has resulted in, or had the potential to result in, a material loss or a significant deviation from expected performance. Operational Risk Events are recorded and analysed to:

- support/provide input to the assessment (quantification) of a specific risk or category of risk.
- indicate a change in the threat level of a particular risk factor.
- provide assurance on the effectiveness of the existing risk response/mitigation actions.
- alert to new / previously unidentified or underestimated risks to ensure the completeness of the business risk profile.

11.3. Risk events are categorised as follows:

- Quantifiable (in terms of impact on profit or net asset value):
  - Loss: which includes loss of sales revenue as well as losses incurred in terms of invalid/inaccurate disbursements of policy/product benefits, loss of tangible assets, increased operating costs, business recovery costs, penalties, interest, compensation, legal liability, litigation costs, internal and external fraud.

- Gain: being the unintended profits made as the result of operational errors.
- Near-miss (quantifiable): where losses, despite the initial potential, are avoided by chance or prevented by compensating controls.

- Non-quantifiable:
  - Incident: negative impact, but not readily quantifiable.
  - Near-miss (non-quantifiable): where losses, despite the initial potential, are avoided by chance or prevented by compensating controls.

11.4. Thresholds for recording of loss incidents

Quantifiable incidents exceeding R10 000 (per event) must be recorded separately. Less-significant quantifiable events under R10 000 will be "summarised / accumulated" per type of event per calendar month and recorded accordingly (with an indication of the number of individual events). The established processes for reporting incidents should be followed Businesses can record events at a finer granularity at their own discretion.

Risk Specialists must take cognizance of all material events suffered by the business, as well as "near-misses" (where actual losses were either avoided by chance or prevented through the effectiveness of controls). Loss and incident trends must be analysed to ensure the completeness of the business risk profiles and associated key risk indicators

12.MONITORING COMPLIANCE WITH THE POLICY

12.1. Formal Self-Assessments:

The Group is required to perform a risk management maturity self-assessment on an annual basis, according to the self-assessment methodology prescribed by Group Risk Management. The Group should review and report on its risk management process accordingly, with the aim to improve the process, and to modify it in the light of changed circumstances.

The focus of the review, and the contents of the report, should be on issues such as:

- The existence, completeness and effectiveness of the risk management process.
- 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.); and
- Whether the risk profile and risk reporting adequately communicate the business' risks to senior levels, in a way that contribute to improved decision-making.
- Areas for improvement in maturity and related action plans must be incorporated into the risk management plans of the Group.

12.2. Independent Assurance:

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 Audit and Risk Committee and other applicable Committees, as well as the Group.

12.3. Annual Risk Plans:

The Risk Management Function must submit their risk plans for the year to Executive Enterprise Risk Committee and the Audit and Risk Committee

13. REPORTING ON POLICY OUTCOMES DISCLOSURES

The Audit and Risk Committee is responsible for mandatory disclosures in relation to risk management in the Group, including disclosures required in terms of the King IV Report in the integrated annual report. It should as a minimum disclose:

- That it is accountable for the process of risk management and the system of internal control, which is regularly reviewed for effectiveness.
- That there is an ongoing process for identifying, analysing, evaluating and managing the significant risks faced by the Group, 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;
- That there is an adequate and effective system of internal control in place to mitigate the significant risks faced by the Group to an acceptable level. Such system is designed to manage, rather than eliminate, the risk of failure or maximizing opportunities to achieve business objectives and can only provide reasonable but not absolute assurance;
- That there is a documented and tested process in place, which will allow the Group 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;
- The Board's view on the effectiveness of the risk management process; and
- Any undue, unexpected or unusual risks.

14. POLICY PROVISIONS

All managers, executives and employees of the Group and its subsidiaries shall ensure that the provision of this policy is read, understood and adhered to.

15. ROLES & RESPONSIBILITIES

Specialist risk management roles exist within the Group. A decentralised risk management philosophy is followed whereby each role has a specific mandate to manage particular risks or to provide assurance on the management of such risk. A detailed summary of the roles and responsibilities is included below.

Specific metrics and management actions must be reported to the Chief Risk Officer to ensure that an overall portfolio view of risk is maintained for the Group.

ROLE	DESCRIPTION
Audit and Risk Committee (ARC)	**The ARC shall** • Address the corporate governance requirements of Enterprise Risk Management • Monitor the Group's performance against the Enterprise Risk Management Policy and Framework. • Monitor the implementation of the Enterprise Risk Management Framework. • Approve the appetite and tolerance for risk.

	• Provide direction and oversight in respect of Enterprise Risk Management. • Ensure that the responsibilities and co-ordination of Enterprise Risk Management are clear. • Ensures that the corporate strategy of the Group is responsive to the risks reflected in the strategic/key risk register. • Advise the Board of Directors on urgent risk management issues and required initiatives as part of its quarterly reporting process. • Oversee the implementation and maintenance of the ongoing process of risk identification, quantification, analysis and monitoring throughout the Group. • Evaluates the material risk profile of the Group Reports to the Board of Directors on the work undertaken and on the actions taken by management to address identified areas for improvement.
Board of Directors	**The Board of Directors shall:** Set the direction for how risk should be approached and addressed in the organisation. This shall encompass: • The opportunities and associated risks to be considered when developing strategy; and the potential positive and negative effects of the same risks on the achievement of organisational objectives. • Treat risk as integral to the way it makes decisions and executes its duties. • Approve policy that articulates and gives effect to its set direction on risk. Evaluate and agree on the nature and extent of the risks that the organisation should be willing to take in pursuit of its strategic objectives. It should approve in particular: • The organisation's risk appetite, namely its propensity to take appropriate levels of risk; and • The limit of the potential loss that the organisation has the capacity to tolerate. • Delegate to management the responsibility to implement and execute effective risk management. Exercise ongoing oversight of risk management and, in particular, oversee that it results in the following:

	• An assessment of risks and opportunities emanating from the triple context in which the organisation operates and the capitals that the organisation uses and affects. • An assessment of the potential upside, or opportunity, presented by risks with potentially negative effects on achieving organisational objectives. • An assessment of the organisation's dependence on resources and relationships as represented by the various forms of capital. • The design and implementation of appropriate risk responses. • The establishment and implementation of business continuity arrangements that allow the organisation to operate under conditions of volatility, and to withstand and recover from acute shocks. • The integration and embedding of risk management in the business activities and culture of the organisation. • Consider the need to receive periodic independent assurance on the effectiveness of risk management. • The nature and extent of the risks and opportunities the organisation is willing to take should be disclosed without compromising sensitive information. Ensure the following is disclosed in relation to risk: • An overview of the arrangements for governing and managing risk. • Key areas of focus during the reporting period, including objectives, the key risks that the organisation faces, as well as undue, unexpected or unusual risks and risks taken outside of risk tolerance levels. • Actions taken to monitor the effectiveness of risk management and how the outcomes were addressed. • Planned areas of future focus
Chief Executive Officer	The CEO is accountable and ultimately responsible for ensuring that all components of Enterprise Risk Management are in place, and **The CEO shall:** • Set the tone at the top that influences internal environmental factors and other components of Enterprise Risk Management. • Take actions concerning the Group's organisational structure, content and communication of key policies and

	the type of planning and risk reporting systems that the Group will use. • Meeting periodically with Senior Managers responsible for major business units and functional areas to review how they manage risk. • Gain knowledge of risks inherent in operations, risk responses and control improvements required and the status of efforts underway clearly defining the information needs. • Ensure the presence of a positive internal environment, more than any other individual or function. Work with senior management to manage risks within the organisation.
Chief Risk Officer	**The CRO shall have the following responsibilities** • Decide on a methodology and framework for Enterprise Risk Management. • Performs reviews of the risk management process to improve the existing process. • Facilitate annual risk management assessments • Ensure a system is in place for risk monitoring and risk improvement. • Aligns the risk assessment and risk identification process with the Group's targets and objectives. • Compile a consolidated strategic risk register on an annual basis. • Provide the audit function with information reflected in the risk registers with the intended purpose of assisting audit in performing their duties where applicable. • Ensures that risk management training is conducted at appropriate levels within the company to inculcate a risk management culture. • Enable the Audit and Risk Committee of the Board to fulfill its responsibilities. • Enables proper risk management ownership by Executives. • Promote the Enterprise Risk Management Framework to the Board. • Ensure that a risk management capability is developed and maintained in all business units and subsidiaries. • Reports to the Audit and Risk Committee regarding the: • Progression of Enterprise Risk Management and its implementation.

	• Identified significant and material risk exposures and recommendations across the Group; and • Consolidated Enterprise Risk Register encompassing analysis and recommendations.
Divisional/BU ERCO	**The BU or Divisional ERCOS shall have the following responsibilities:** • Implementation of Enterprise Risk Management methodologies and processes in line with the Group's ERM Framework within their business units. • Identifying, evaluating and reviewing specific operational risks, assessing their impact and probability, assigning risk owners and defining actions to address the risks. • Reviewing and updating the business unit risk registers and the risk management system. Escalating all material issues and significant risks to the EERCO through the appointed Risk Management Champion to the Risk Management Department.
Employees	All employees, staff, managers and directors in the Group and its subsidiaries have responsibility for Risk Management.
Executive Committee (EXCO)	**The Executive Committee (EXCO) shall :** • Be accountable to the Board of Directors for designing, implementing and monitoring the process of risk management and integrating it into the day-to-day activities of the Group. • Deciding on the manner in which risk mitigation will be embedded into management processes. • Inculcating a culture of risk management in the Group. • Viewing risk as an opportunity by applying the risk/ reward principle in all decisions impacting upon AHL Group. • Assigning a manager to every key risk for appropriate mitigating action and to determining an action date. • Ensuring that adequate and effective risk management structures are in place. • Identifying, evaluating and measuring key risks and where possible quantifying and linking each identified risk to strategic objectives. • Defining the roles, responsibilities and accountabilities at the executive and management level
Executive Enterprise Risk Committee (EERCO)	**The Executive ERCO shall have the following responsibilities:**

	• Reviewing the Group's Risk Profile. • Reviewing performance measures against tolerances and recommending corrective action where appropriate. • Communicating to the Audit and Risk Management Committee. • Determining risk management delegation of responsibility and authority. • Reviewing the adequacy and overall effectiveness of the Enterprise Risk Management process in the Group and its implementation by management and ensuring that appropriate action is taken to mitigate risks. • Ensuring that a risk-based approach is incorporated into the Group's business units and subsidiaries for key decision-making purposes. • Ensuring compliance with risk Enterprise Risk Management Framework, risk management strategies and policies, and procedures. • Ensuring that risk policies are formally reviewed. • Monitoring the implementation of the Enterprise Risk Management Framework. • Ensuring that group policies are approved
Internal Audit	**Internal Audit shall have the following responsibilities:** • Providing assurance that management processes are adequate to identify and monitor significant risks. • Using the outputs of risk assessments to direct internal audit plans. • Providing ongoing evaluation of the risk management processes. • Providing objective confirmations that the Board of Directors receives the right quality of assurance and reliable information from management regarding risk. • Providing assurance regarding Enterprise Risk Management processes from both a design and functional perspective. • Providing assurance regarding the effectiveness and efficiency of risk responses and related control activities; and • Further providing assurance as to the completeness and accuracy of Enterprise Risk Management reporting. • Assume the responsibility of implementing the combined assurance frameworks, procedures and coordinating key combined assurance activities.

Risk Management Function	• The Group Risk Management Function provides a second line of defence, engaging with management in implementing the Enterprise Risk Management Framework and applicable policies and methodologies and systems whilst providing constructive challenge and oversight. • The Group Risk Management Function does not directly manage risk – this is the responsibility of the business units that generates the risk in the first place. • It is ultimately answerable to the Audit & Risk Committee and Board for the effectiveness of discharging this role. • The Group Risk Management Function shall be responsible for establishing, implementing and maintaining appropriate mechanisms and activities to: • Support the Board and management in articulating and reviewing its risk appetite. • Cascade risk appetite, tolerances and limits across the business from group down to entity level and ensure active monitoring of risk exposures versus tolerance limits. • Facilitate identification and assessment of the risks that the Group and its subsidiaries faces. • Establish and maintain an aggregated view of the risk profile of the Group. • Ensure that accountabilities for risk management are appropriately embedded into management's Key Performance Areas and roles and responsibilities. • Regularly report to set governance structures on the Group's risk profile, and details on the risk exposures facing the Group and related mitigation actions as appropriate. • Document and report material adverse changes affecting the Group's risk management system to Group Executive Committee and to the Board of Directors to help ensure that the framework is maintained and improved. • Support management in embedding a risk management culture by providing risk management awareness, training and development programs tailored to the business's requirements. • Assist the Board of Directors and Senior Management in carrying out their respective responsibilities, including by providing specialist analysis and performing risk reviews.
Senior Managers/Managers	• Promote compliance with the risk appetite • Manage risks within their areas of responsibility consistent with risk tolerances.

Annexure A:

Afrocentric Risk Rating Table 1. Purpose of the Risk Rating Table The purpose of the Risk Rating Table is to ensure that significant risks and incidents are escalated consistently to the appropriate level of management and assurance oversight within the Group.

Although the actual management of a risk event will in most instances remain with the (senior & executive) management and board of the business, the Executive Enterprise Risk Committee and the Group Exco can decide to intervene, i.e., to request active involvement from the Chief Risk Officer , as well as through regular and/or additional monitoring In addition, the purpose of the Risk Rating Table is to ensure consistency and to enable suitable aggregation of risks and incidents at Group Level.

2. Determining the Likelihood The likelihood or probability of an event occurring is rated on a 6-point scale.

	Likelihood rating	Approximate probability of risk materialising
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% plus

3. Determining the Impact at Group Level The impact is defined as the potential loss to the Group or Business Unit, financial or otherwise, should the risk materialise. It is the residual impact after considering the foreseen effectiveness of the relevant mitigation measures currently in place. Furthermore, the residual risk qualification must be reflected gross of any insurance claim(s) under an insurance policy covering such risk. Amounts recoverable should be reflected separately, indicating the nature of the insurance claim / contract.

Where it is not possible to readily estimate the financial impact of a risk, a common-sense approach should be followed to assign an appropriate threat level.

Impact on:		Approximate impact of risk materialising to the Group
1	Insignificant	0% to <1%
2	Minor	1% to <5%
3	Moderate -	5% to <20%
4	Moderate +	20% to <50%
5	Major	50% to <80%
6	Extreme	80% plus

4. Determine the Significance of the Risk

The significance of the risk is determined by charting the foreseen impact and probability of the risk materialising on the following grid.

Type of risk or loss event			Likelihood					
			1	2	3	4	5	6
			Rare <1%	Unlikely <5%	Possible- <20%	Possible+ <50%	Likely <80%	Almost certain >80%
Impact	6	Extreme	M	M	H	VH	VH	VH
	5	Major	M	M	H	H	VH	VH
	4	Moderate+	L	M	M	H	H	VH
	3	Moderate-	L	M	M	M	H	H
	2	Minor	L	L	M	M	M	M
	1	Insignificant	L	L	L	L	L	M*

Subject to minimum impact amount of R5m