Risk Management Strategy, Methodology & Approach

RMS_GRC_001

Version 6.0 December 2020

Version Control and Approval

Document Name	Risk Management Strategy, Methodology and Approach
Document Number/Version	6.0

Implementation

Implementation Date	2021/22 Financial Year

Approval

Date Approved	June 2021
Related Documents	Risk Management Framework, Risk Management Policy, Risk Management Implementation Plan

Compiled by: Governance, Compliance & Risk (Nthabeleng Ngoepe, Ebrahim Mayet and Bopila Kadi)

Reviewed by Statutory Reporting, Risk, Governance and Compliance Manager

Name: Mompoloki Olenle

Signature:

Reviewed by CFO

Name: Ikalafeng Diale

Signature: Date:

Recommended by CEO

Name: Thamsanqa Mdontswa

Signature: Date:

Recommended by RMC

Name: Bhekokwakhe Henry Gutshwa

Signature: Date: 14.07.2021

Recommended by ARC

Name: Michelle P Ilay: ARC Chairperson

Position: Chairperson: Audit and Risk Committee

Signature: Date:

Approved by the Board on 17 June 2021.

Name: Chris Mudau

Position: Chairperson of the Accounting Authority

Signature: Date:

Contents

1. INTRODUCTION 4
2. SCOPE 5
3. RISK MANAGEMENT TOOLS AND TECHNIQUES 5
4. ENTERPRISE RISK MANAGEMENT FRAMEWORK 8
5. RISK TREATMENT 11
6. SASSETA's RISK PROFILE 12
7. ENTERPRISE RISK MANAGEMENT (ERM) OBJECTIVES 12
8. CONTINUOUS IMPROVEMENT 17
9. RISK MANAGEMENT STRUCTURE AND REPORTING LINES 19
10 POLICY REVIEW 20

1. INTRODUCTION

SASSETA's strategic objectives can be achieved by managing or reducing risks and enhancing the quality of Management decision-making through proper planning and optimal allocation of the organisation's resources. This Strategy outlines the activities that the Governance, Risk and Compliance Unit shall implement, support and ensure the successful implementation of SASSETA's Risk Management Policy and the Risk Management Implementation Plan.

Enterprise Risk Management defines the decisions, the involvement by various stakeholders, and the structures, processes, responsibilities and other mechanisms required to make decisions. This involves building the right capacity, processes and structures in order to make relevant decisions that achieve alignment, manage risks, improve business performance and manage costs.

1.2 Enterprise Risk Management is implemented in accordance with the ISO 31000 Standard and the King IV Report as outlined below:

1.2.1 ISO 31000 Standard

The Standard contains a systematic and logical way of dealing with the risk management function and activities. The process outlines how SASSETA shall manage risks by anticipating, understanding and mitigating risks which have been identified. The process further indicates the importance of communicating and consulting with stakeholders and monitoring, reviewing and reporting the risks and their related controls.

1.2.2 King IV

King IV emphasizes that the Board should appreciate that strategy, risk, performance and sustainability are inseparable. It also provides that the Board is responsible for governance of risk and should ensure that there is an effective risk-based Internal Audit. Therefore, the Board must ensure that ERM is embedded in the governance processes of the organization, in order to achieve performance through the effective and efficient provision of services.

King IV also advises on the following issues regarding risk management:

- Risk governance;

- Risk appetite and tolerance;
- Linking performance and risk management;
- Compliance risk;
- Combined Assurance Framework;
- Fraud risk; and
- ICT Governance.

All the above factors have been taken into account in the development of the Risk Management Framework, Risk Management Implementation Plan and the Risk Management Policy.

2. SCOPE

The Risk Management Strategy, Methodology and approach applies to SASSETA's Board and governance structures, the Chief Executive Officer and all employees.

3. RISK MANAGEMENT TOOLS AND TECHNIQUES

3.1 Risk Management Policy

PFMA Section 51 (a) (i) states that the Accounting Authority must ensure that a public entity has and maintains effective, efficient and transparent systems of financial and risk management and internal control.

The Risk Management Policy outlines SASSETA's commitment to the effective and efficient promotion and management of stakeholder value and undertakes to do so in a way that; minimizes exposure that could adversely impact on its reputation and ability to fulfill its legislative mandate.

The Accounting Authority ensures that there is effective and efficient risk management in the SETA and that the ERM methodology and techniques are embedded within strategy setting, planning and business processes to safeguard performance and sustainability. The rigors of risk management provide responses and interactions that strive to create an appropriate balance between risk and reward.

3.2 Risk Management Framework

Greater emphasis and guidance on how risk management should be implemented and integrated into the organization is guided by the Risk Management Framework, which is based on the ISO 31000 Standard and National Treasury's Public Sector Risk Management Framework. Thus, the Governance, Risk and Compliance Unit follows guidelines and principles from the Standard in order to achieve effective risk management implementation.

3.3 Combined Assurance Plan

Combined Assurance establishes an integrated and coordinated approach and assists the Accounting Authority in assessing whether the organization is able to execute its strategies successfully in order to achieve its organizational objectives. This is achieved through the establishment of the Combined Assurance Plan.

Combined Assurance focuses on all assurance processes regarding the key risks facing the SETA in an integrated manner, such that they complement one another in their efforts to ensure the mitigation of the SETA's risks. Combined Assurance defines three assurance levels i.e. Management, Oversight Functions and Independent Assurance Providers, including External Audit.

By effectively implementing Combined Assurance a number of benefits can be realized, including, amongst others:

- More coordinated and relevant assurance efforts focusing on key risk exposures;
- Minimizing business or operational disruptions;
- A comprehensive and prioritized approach in tracking of remedial actions on identified improvement opportunities or weakness;
- Improved reporting to the Accounting Authority;
- A possible reduction in assurance costs;
- Minimizing duplication of effort; and
- Reliance on work performed by other assurance providers.

3.4 Fraud Prevention Policy and Plan

SASSETA is committed to preventing fraud and corruption from occurring and to create an anti-fraud culture. To achieve this, SASSETA undertakes to comply with the relevant requirements of the Public Finance Management **Act** (**PFMA**), 1999 (**Act** No. 1 of 1999) (as amended by **Act** No. 29 of 1999), National Treasury Practice Notes and the principles of corporate governance. The Fraud Prevention Policy is intended to:

- Define fraud and highlight duties and responsibilities of the Board,, Board sub-committees, Management and all employees of SASSETA;
- Develop and maintain effective internal controls to prevent fraud;
- Ensure that when fraud occurs, vigorous and prompt actions are undertaken;
- Prevent and detect instances of fraud, theft, and misappropriation of SASSETA's assets and resources;
- Assign responsibilities for the development, implementation and monitoring of fraud prevention mechanisms;
- Communicate the channels of the reporting of economic crimes;
- Create an awareness and obtain cooperation from management, employees and third parties in the prevention and detection of fraud within SASSETA;
- Define SASSETA's response to fraudulent incidents;
- Recover financial losses incurred by SASSETA as a result of perpetrated fraud; and
- Prevent fraud through an effective implementation of the Fraud Prevention Plan.

3.5 Key Risk Indicator Guidelines

3.5.1 The purpose of Key Risk Indicators (KRIs) is to develop a tool within Enterprise Risk Management (ERM) to facilitate the monitoring and control of risk. This shall be used to support risk management activities and processes, including risk identification, risk and control assessment, and implementation of risk appetite. Key risk indicators can be used in the management of operational risk, also in a wider context in the overall management of SASSETA operations.

The KRIs are metrics used to monitor identified risk exposure over time. It is a measurement tool that indicates the following:

- Amount of exposure to a given risk;
- Emerging risk;

- Effectiveness of mitigating controls;
- Whether a risk has occurred or could eventuate;
- How well the risk exposures are being managed; and
- Risk escalation or re-prioritization.

3.5.2 Comparison **between Key Risk Indicators (KRI) and Key Performance Indicators (KPI)**

Key Risk Indicators are measurement tools used to assist management to identify and correct emerging risks or determine where risks have materialized or not, and then implement corrective measures at an early stage, while Key Performance Indicators help management understand how well their departments are performing in relation to their strategic goals and objectives. Key Performance Indicators provide the most important information that enables SASSETA to understand whether the organization is on track or not.

3.6 Risk Appetite and Tolerance (RAT) Framework

In line with the Public Sector ERM Framework and ERM Strategy, Methodology and Approach adopted by SASSETA, it is the responsibility of SASSETA to establish a clearly stated and articulated risk appetite in the various areas of operation to inform management decisions. A risk appetite is critical, as it is a driver of strategic risk decisions at Board level. At Executive level it translates into a set of procedures to advise tactical decisions and at an operational level, it dictates for routine activities.

The Accounting Authority set SASSETA's risk appetite level at **14**. The appetite level can be adjusted from time to time depending on the organizations risk maturity level, as articulated in SASSETA's Risk Management Procedures.

4. ENTERPRISE RISK MANAGEMENT FRAMEWORK

The Risk Management Process provides a description for the approach taken to identify and manage the risks associated with the organisation. The approach is

informed by the Risk Management Process outlined in the Public Sector Risk Management Framework and ISO 31000. SASSETA's risk management process is depicted on Figure 1 below.

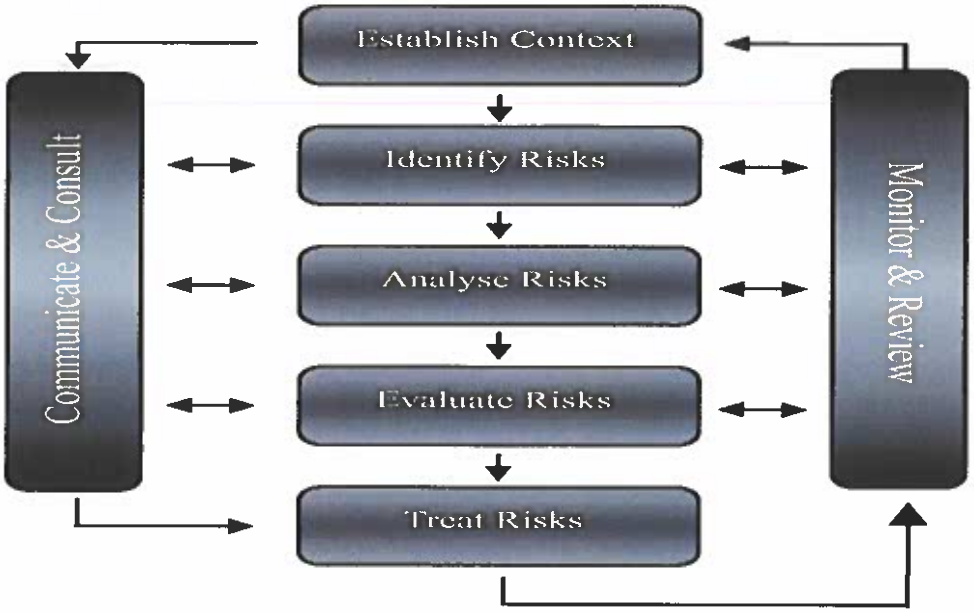


Figure 1: SASSETA's risk management process

4.1 **Understanding of the Corporate Plan** (Establish Context)

The risk context may be summarized as follows:

The External Context: All external factors that are taken into account in risk management, like laws and regulations, contracts, trends in business drivers, political and socio-economic factors.

The Internal Context: These are all internal factors that are taken into account, like capabilities, resources, people, business processes, systems, policies to ensure that the gap between Executive Managers, Managers and staff members in the organization is minimized. Therefore, organizational objectives are then used to give effect to context and risk criteria.

4.2 **Development of Risk Profiles** (Identify, Analyze and Evaluate Risks)

The development of a Risk Profile involves the following three tasks:

- Risk identification, i.e. all risks associated with a decision must be identified and placed in a risk register;
- Risk analysis - the purpose of risk analysis is to provide the decision maker with sufficient understanding of the risk;
- Risk evaluation - Each risk once analysed is evaluated by comparing the residual risk after risk treatment or with existing controls.

The risk evaluation phase is used to make a decision concerning which risks need treatment and the treatment priorities based on the foregoing analysis. SASSETA uses the following **risk evaluation matrix**:

IMPACT						
	5 Critical	5- Low	10 medium	15 high	20 high	25 high
	4 Major	4- Low	8 medium	12 medium	16 high	20 high
	3 Moderate	3- Low	6 medium	9 medium	12 medium	15 high
	2 Minor	2	4 low	6 medium	8 medium	10 medium
	1 Insignificant	1	2 low	3 low	4 low	5 low
		1 Rare	2 Unlikely	3 Moderate	4 Likely	5 Common
	Likelihood					

Risk Rating= *impact x likelihood*	**Risk Magnitude**	**Definition**

15- 25	High	Immediate action required at Senior Management level
6-14	Medium	Management responsibility must be specified
1-5	Low	Managed by routine procedure

5. RISK TREATMENT

5.1 **Ongoing Management of Risks** (Risk Treatment)

Risk treatment involves the identification of control options, selection of a control options and implementation of a control option. There are four (4) risk treatments that can be selected to mitigate against a particular risk namely:

- Avoid – an activity in order to not to be exposed to a particular risk;
- Transfer – form of risk treatment involving the agreed distribution of risk;
- Accept – informed decision to take a particular risk;
- Reduce – process that is modifying risk.

5.2 **Monitoring and Reporting** (Monitor, Review, Communicate and Consult)

Consistent with ISO 31000, every aspect of the risk management process shall be monitored and reviewed, including:

- Has the risk changed in character and are there new risks emerging;
- Has the context for risk management changed;
- Is the risk treatment plan being implemented as planned;
- Are controls effective;
- What is the appropriate frequency of monitoring;
- Was the risk assessment accurate based on the objectives;
- Can monitoring be improved by identifying better key performance indicators and key risk indicators; and
- Has management KPIs been updated to reflect as their function.

6. SASSETA's RISK PROFILE

The value of the Risk Management Analysis Approach derives from the diversity of participants, the quality of the facilitated discussions and the consensus of decisions arrived at. The Governance, Risk and Compliance Unit facilitated discussions and workshops with MANCO (Management Committee) and practitioner representatives for each Business Unit, following which the Risk Profile below was developed.

The objective of developing a risk profile is:

- To evaluate the risks and develop a risk register that can be used for effective risk reporting and monitoring of SASSETA's risk exposure;
- To enable Management to prioritize their risk management efforts towards the development and implementation of the SETA's objectives; and
- To be able to identify risk mitigation plans related to the SETA.

7. ENTERPRISE RISK MANAGEMENT (ERM) OBJECTIVES

In response to the Strategic Plan and the analysis of the SETA environment, the Governance, Risk and Compliance Unit developed objectives which outline how ERM will be implemented and how the foreseeable risks will be managed in a manner which is proactive, effective and appropriate, in order to assist SASSETA to achieve its objectives, while maintaining risk exposure at an acceptable level.

The ERM objectives focus on the consequential and significant risk to SASSETA's mandate. This outlines Management's view on the most consequential risks the organization faces, their likelihood, their potential effect, the frequency, the nature of updating the identification of such top risks and the role of risk management in strategic decision making.

Risk is associated with human error, system failures and inadequate procedures and controls. Risk Management provides risk controls which provides good management practices and involves consistent alertness and continuous improvement. This is a value-adding risk management activity that impacts, either directly or indirectly on bottom-line performance.

It must be borne in mind that risk management is ultimately the responsibility of the Accounting Authority and, therefore, the objectives were developed on the premise that the Governance structure of the Accounting Authority is in place to deal with ERM.

7.1 Provide an Effective and Efficient ERM Infrastructure

7.1.1 Establish Risk Management Committee (RMC)

SASSETA has established a Risk Management Committee (RMC), which is responsible for assisting the SETA in the effective discharge of its accountability for Risk management by reviewing the effectiveness of the SETA's risk management systems, practices and procedures, and providing recommendations for improvement.

7.1.2 Ensure optimized utilization of the ERM Information System

The ERM Department continuously implements a Risk Management Tool (GRC) which consists of Risk Management, Governance and Compliance. The main benefits of the tool are integration between the three modules, information repository and reporting functionalities.

Upon successful procurement, the ERM information system should be able to provide the following benefits

- Provide an all-encompassing view of the organization risk universe;
- Streamline controlled management of risk, which allows process owners to direct responsibility for managing controls;
- Facilitate the tracking of action plans to address any identified loss events, enterprise risks, deficient controls, including automated notifications and reminders together with security-based work-flow process;
- Interact with insightful risk dashboards, which give enterprise wide visibility and highlight issues that need to be addressed; and
- The ERM Information System should, upon procurement, function at all levels, strategic, managerial and operational, allowing the fostering of a culture of responsibility and continual improvement, with clear visibility of performance against strategic objectives.

7.1.3 Develop and Implement Risk Appetite and Tolerance Framework

The Risk Appetite and Tolerance Framework has been developed for implementation as a guide for Executive Management to define and set risk tolerance levels as per the current Strategic Plan. The defined risk tolerance levels shall be used to manage risks across the SETA.

As stated in the ERM Framework, it is the responsibility of the Accounting Authority / Board to establish the risk appetite. In accordance with the provision of PFMA, SASSETA shall have a low appetite for all forms of loss resulting from negligence, wasteful and fruitless expenditure.

7.2 Instill Risk Culture Across SASSETA

7.2.1 Risk Training and Awareness Programme

Risk training shall regularly be conducted across SASSETA as per the Risk Management Implementation Plan. As part of the risk profiling exercise within SASSETA, the Governance, Risk and Compliance Unit shall from time to time conduct risk awareness sessions with all staff. This process is to continue ensuring an increase in maturity level for risk management at all organisational levels.

7.2.2 The following key elements shall be implemented in order to develop a strong risk culture within SASSETA:

- **Strong support from the Accounting Authority and Management**

  The Accounting Authority is responsible for setting the stage for culture change and establishing the vision and organization wide rules and guidelines related to risks. The roles and responsibilities of the Accounting Authority, Executive Management, Management and all employees from a risk management point of view shall be strengthened and clarified.

- **Accountability and ownership**

  The Board is ultimately accountable for risk management within SASSETA. Through the Audit and Risk Committee (ARC) and the Risk Management Committee (RMC), the Board shall ensure compliance to the ERM Strategy, Methodology and Approach, Policy and Framework..

  The Board and Management shall review and approve the risk appetite from which Governance, Risk and Compliance Unit shall engage Management across

SASSETA in dialogue on risk implications on business strategies. Management shall consider the risks in the recruitment process and adhere to clear communication and understanding of business expectations and performance measurement implications.

- **Risk transparency**

This element ensures that risk positions are consistent with the risk appetite and are understood by the risk owners. Risk reporting, risk dashboard and risk analytics shall be improved. Risk discussion forums at Senior Management level have been created, to promote a culture of performance.

- **Communication and training**

Risk appetite being communicated across the organization for a better understanding of risks pursued by risk owners. The Governance, Risk and Compliance Unit and the Human Resources Department shall jointly create workshop programs to increase knowledge and understanding of risk throughout SASSETA.

- **Risk-adjusted Return on Capital Optimization**

Engage Management to put risk at the center of discussions during periodical strategic planning and to consider risk-return as an integral part of decision making.

- **Partnership and collaboration**

Improve cooperation and dialogue with risk owners to enable the pursuit of sustainable growth opportunities. The Governance, Risk and Compliance Unit shall work proactively with Management to establish trust and open conversation about risk related issues and ensure that risk information is shared with business lines. The Governance, Risk and Compliance Unit in consultation with MANCO shall also establish Risk Champions and Risk Coordinators across SASSETA.

7.3 Embed Risk Management within daily operations of SASSETA

7.3.1 Facilitate Risk Assessments across the organization

Development and Management of strategic and operational Risk Profiles, at departmental levels through assessments is very critical. The management of these risk profiles is guided by the Risk Management Policy and ERM Framework. This will be outlined in the ERM Implementation Plan.

7.3.2 Develop Risk Mitigation Strategies

The Governance, Risk and Compliance Unit shall assist Management to develop adequate and effective mitigating controls in order to manage risks properly. Internal audit shall develop its internal audit plan on the basis of the key risks identified. The internal audit function shall provide an independent, objective assurance on the effectiveness of the system of risk management, and on the adequacy and effectiveness of the adopted controls.

7.4 Empower SASSETA to proactively respond to project risks

Project Risk Management delivers a number of values, including producing better business outcomes through more informed decision making, having a positive influence on creative thinking and innovation, creating better project control and contributes to project success. This shall also provide guidance to the Risk Manager, Project Managers and Project Stakeholders on the application of standard risk management processes for all business programs and projects within SASSETA.

Significant projects which have an impact on the successful implementation of business objectives shall be identified and the risk management process has been embedded as part of the project management process. This assist in ensuring that Project Managers manage risks within their projects as per the ERM Framework and Strategy.

For significantly material business projects, a Project Management Plan, defining the following shall be developed and maintained:

- Risk Management methodology to be used;
- Assumptions that have a significant impact on a project;
- Roles and responsibilities unique to the risk management function;
- Risk Management milestones;

- Risk rating techniques;
- Risk thresholds;
- Risk communication; and
- Risk tracking processing.

7.5 Improve Risk Management Reporting

7.5.1 Identified risks shall be reviewed and updated on a monthly basis, and this process enables Management to identify new risks as soon as possible, decide where and how to handle those risks and look for other risks that might be reduced or eliminated and no longer require coverage.

7.5.2 To ensure integration and alignment of assurance processes in SASSETA and to maximize governance oversight and control efficiencies, a Combined Assurance Plan has been developed and implemented. The purpose of a Combined Assurance Plan is to optimize the assurance to the Accounting Authority, the Audit and Risk Committee (ARC) and the Risk Management Committee (RMC) by Management, internal assurance providers and external assurance providers on the risk areas affecting the SETA. To coordinate the appropriate level of assurance or controls over significant risk areas identified by the organization and to provide appropriate reports.

7.5.3 The ERM Information system should provide a structured and systematic approach to manage risks across the organization. It does so by creating a central platform for an integrated Combined Assurance Model based on technological innovation. The technology should be able to develop and provide solutions that support the organization processes and methodologies.

8. CONTINUOUS IMPROVEMENT

8.1 The Governance, Risk and Compliance Unit is required to conduct periodic reviews of the risk management system in order to ensure its continuing stability and

effectiveness in satisfying requirements of SASSETA's Strategic Objectives. Records of such reviews shall be maintained.

8.2 Continuous Risk Management Steps

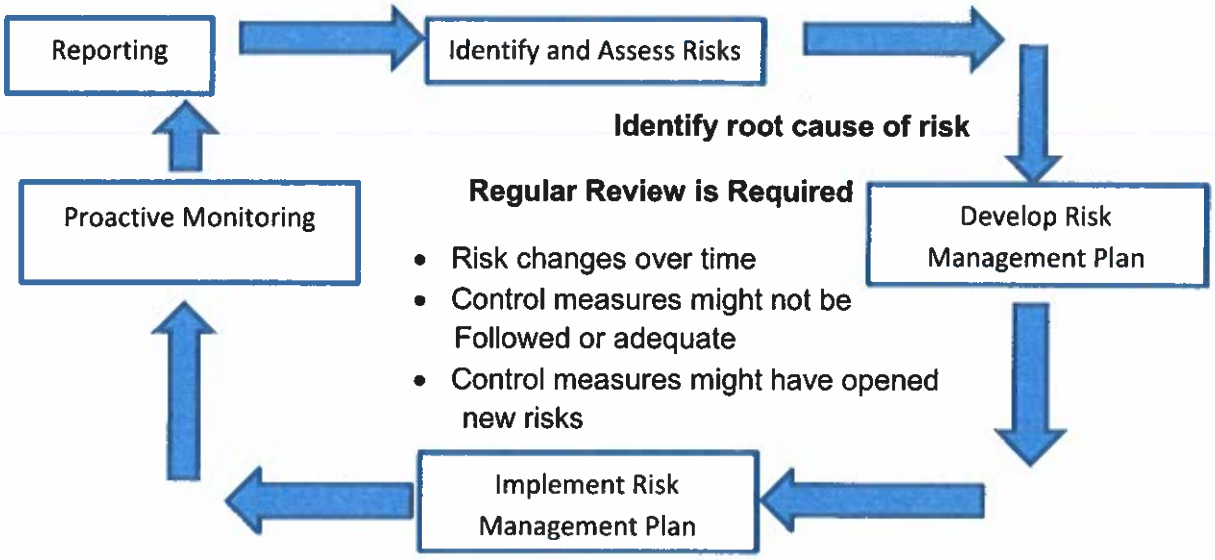
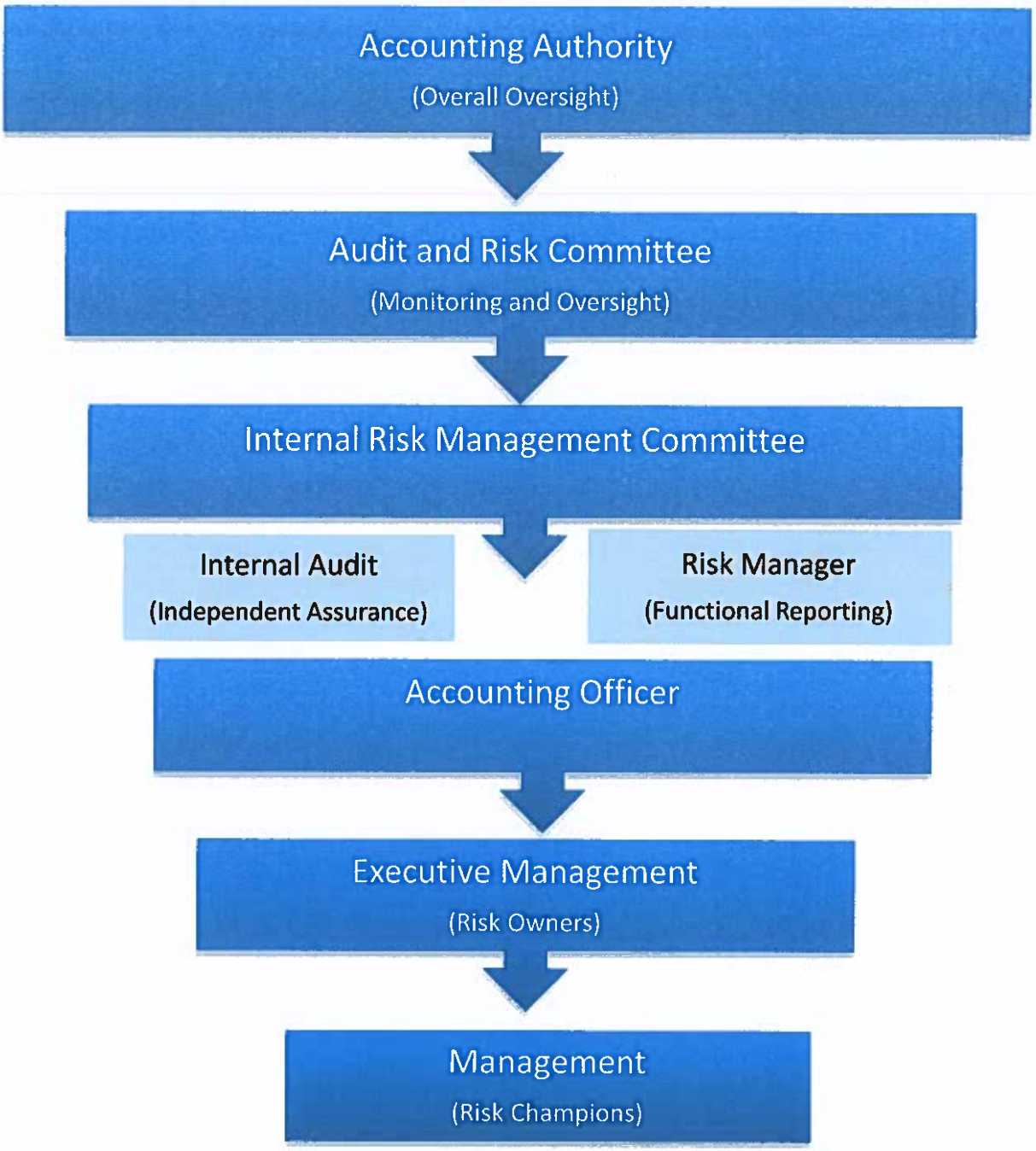


Figure 2: Continuous risk management steps

9. RISK MANAGEMENT STRUCTURE AND REPORTING LINES



10 POLICY REVIEW

This Policy shall be reviewed every two years or when Management or any relevant governance structure deems it fit for continuous control and monitoring of the regulatory environment for possible amendments and recommendation to the Accounting Authority / Board for approval.