

PROVINCE OF THE EASTERN CAPE



DEPARTMENT OF RURAL DEVELOPMENT AND AGRARIAN REFORM

ENTERPRISE RISK MANAGEMENT FRAMEWORK AND POLICY

May 2023

Table of Contents

ACRONYMS	iv
DEFINITION OF TERMS AND CONCEPTS	v
FOREWORD.....	vii
1. INTRODUCTION.....	1
2. BACKGROUND.....	2
3. REGULATORY FRAMEWORK	2
3.1 CONSTITUTIONAL MANDATE	2
3.2 PFMA AND TREASURY REGULATIONS	2
3.3 ADDITIONAL LEGISLATION	3
3.4 BEST PRACTICES	3
4. OBJECTIVES	4
5. OWNERSHIP OF RISK MANAGEMENT	4
6. APPROACH: PROCESS FRAMEWORK.....	5
6.1 CREATING AN ENABLING/INTERNAL ENVIRONMENT / INTERNAL ENVIRONMENT	5
6.2 OBJECTIVE SETTING	7
6.3 EVENT IDENTIFICATION	7
6.4 RISK ASSESSMENT	9
6.5 RISK RESPONSE	10
6.6 CONTROL ACTIVITIES: DESIGNING CONTROL ACTIVITIES TO MITIGATE RISKS 10	
6.7 COMMUNICATION AND REPORTING	11
6.8 MONITORING	11
7 RISK APPETITE AND RISK TOLERANCE	11
8 INTEGRATION OF RISK MANAGEMENT ACTIVITIES	12
9 SCOPE OF THE POLICY	12
10 IMPLEMENTATION PROCEDURES: RISK MANAGEMENT STRATEGY AND IMPLEMENTATION PLAN	13
11 ROLES, RESPONSIBILITIES AND GOVERNANCE	13
11.1 EXECUTIVE AUTHORITY	13
11.2 ACCOUNTING OFFICER	14
11.3 AUDIT COMMITTEE	14
11.4 INTERNAL AUDIT	15
11.5 RISK MANAGEMENT COMMITTEE	15
11.6 CHIEF RISK OFFICER	15

11.7	MANAGEMENT	16
11.8	RISK OWNERS	17
11.9	OTHER EMPLOYEES	17
11.10	RISK CHAMPIONS	18
11.11	EXTERNAL AUDIT	18
12	COMPILATION AND MAINTENANCE OF RISK REGISTERS	19
13	RESOURCE IMPLICATIONS	19
14	RISK MANAGEMENT MATURITY	19
15	REPORTING	20
16	EVALUATION OF RISK MANAGEMENT EFFECTIVENESS	20
17	REVIEW OF POLICY	23
18	RECOMMENDATIONS AND APPROVAL OF POLICY	24

ACRONYMS

AO – Accounting Officer

CAE – Chief Audit Executive

COSO – The Committee of Sponsoring Organisations, of the Treadway Commission

CRO – Chief Risk Officer

ERM – Enterprise Risk Management

FMCM – Financial Management Capability Maturity Model

MEC – Member of Executive Council

PFMA – Public Finance Management Act, Act 1 of 1999 as amended

PPT – Provincial Planning and Treasury

RMC – Risk Management Committee

SMS – Senior Management Services

TR – Treasury Regulations, issued in terms of the PFMA

DEFINITION OF TERMS AND CONCEPTS

Definitions – In this Policy, unless the context indicates otherwise mean:

Risk – is the possibility that an event will occur and adversely affect the achievement of objectives.

Enterprise risk management – A continuous, proactive and systematic process, effected by a department's executive authority, accounting officer, management and other personnel, applied in strategic planning and across the department, designed to identify potential events that may affect the department, and manage risks to be within its risk tolerance, to provide reasonable assurance regarding the achievement of the department's objectives

Key Risks – Risks which the organisation perceives to be its most significant risks

Key Risk Indicators – is a measure used to indicate how risky an activity is thus it also serves as an early warning on risks

Leverage - the ability to influence a system, or an environment, in a way that multiplies the outcome of one's efforts without a corresponding increase in cost

Risk Appetite – The level of risk that the organisation is prepared to accept without further mitigation action being put in place, or the amount of risk an organisation is willing to accept in pursuit of value

Risk Architecture – includes the roles, responsibilities, organisation and arrangements for ensuring that risk management receives appropriate attention

Risk Financing – Provision of funds to meet the cost of implementing risk treatment and related costs

Risk Profile – The department has an inherent and residual risk profile. These are all the risks faced by the department, ranked according to a risk matrix. The Risk Score is determined by multiplying the likelihood and impact of the risk.

Risk Register – A formal listing of risks identified, together with the results of the risk analysis, risk evaluation procedures together with details of risk treatment, risk control, risk reduction plans

RISK STAKEHOLDERS

Chief Risk Officer (CRO) – the head of the Risk Management Unit

Risk Champions – The risk champions assist the CRO in the fulfilment of his/her duties. These persons can be in line management in the department but have an alternative reporting line to the CRO or report directly to the CRO.

Enterprise Risk Management Framework and Policy

Risk Owners – A person or entity that has been given the authority to manage, monitor and control a particular identified risk and is accountable for doing so.

Stakeholder – any individual, group or organisation that can affect, be affected by, or perceive itself to be affected by a risk

TERMS RELATED TO RISK ASSESSMENT & MITIGATION

Inherent Risk – The risk to an organisation in the absence of any action management might take to alter either the risk probability or impact

Risk Analysis – Systematic use of information to identify sources and to estimate the risk

Risk Intelligence (RQ) – is the ability of an organization to gather information that will successfully identify uncertainties in the workplace.

Residual Risk – The level of risk remaining after risk treatment

Risk Matrix – The numbers of levels of probability and consequences chosen against which to measure risk.

Risk Optimisation – Process, related to a risk to minimise the negative and to maximise the positive consequences and their respective probabilities

TERMS RELATED TO RISK TREATMENT AND CONTROL

Risk Acceptance – Decision to accept a risk

Risk Avoidance – Decision not to become involved in, or action to withdraw from, a risk situation

Risk Retention – Acceptance of the burden of loss, or benefit of gain, from a particular risk

Risk Reduction/Mitigation – Actions taken to lessen the probability of negative consequences or both, associated with a risk

Risk Transfer - Sharing with another party the burden of loss or benefit of gain, for a risk

Risk Treatment – Process of selection and implementation of measures to modify risk

FOREWORD

As the Department of Rural Development and Agrarian Reform, we are committed to a process of risk management that is aligned to the principles of good corporate governance, as supported by the Public Finance Management Act (PMFA), Act 1 of 1999 as amended and various other pieces of legislations applicable to the Department.

Risk management is recognised as an integral part of responsible management and the Department therefore adopts a comprehensive approach to the management of risk. The features of this process are outlined in the department's Risk Management Strategy. It is expected that all programmes/components and operations work together in a consistent and integrated manner, with an overall objective of reducing risk, as far as reasonably practical.

Effective risk management is imperative to the Department to fulfil its mandate, the service delivery expectations of the public and the performance expectations within the Department. The realisation of our Strategic Plan depends on all employees being able to take calculated risks in a way that does not jeopardise the interest of stakeholders. Sound management of risk must enable the Department to anticipate and respond to changes in its environment, as well as taking informed decisions under conditions of uncertainty.

The departmental staff must adhere to the fundamental principles that all resources must be applied economically to ensure:

- a. The highest standards of service delivery;
- b. A management system containing the appropriate elements aimed at minimising risks and costs in the interests of all stakeholders;
- c. Maintaining an environment, which promotes the right attitude and sensitivity towards internal and external stakeholders' satisfaction;
- d. Educating and training of all staff to ensure continuous improvement in knowledge, skills and capabilities, which facilitate consistent conformance to the stakeholders' expectations.

No organisation operates in a risk-free environment, and no risk management process can guarantee such an environment. Risk management assists organisations to:

- i. Avoid certain adverse outcomes through taking proactive steps (fraud risk prevention, etc.)
- ii. Help institutions cope when actual incidents do occur (disaster recovery plan, business continuity plan, etc.)
- iii. Identify opportunities for continuous improvement.

Through the above, effective risk management therefore assist the department to achieve its performance and service delivery targets, and to reduce the potential loss of resources. This results in effective responsibility and accountability of structures, the improvement of the format used to report performance, and compliance with laws

and regulations, thus avoiding damage to its reputation and other consequences. Additional key benefits include:

- a. Increasing probability of achieving objectives;
- b. Aligning risk appetite and strategy;
- c. Enhancing risk response decisions;
- d. Reducing operational surprises and losses;
- e. Identifying and managing multiple and cross-enterprise risks;
- f. Seizing opportunities;
- g. Ensuring proper financial and asset management;

As can be seen from the above, by being proactive and energetic in the embedding of the risk management process, there are many benefits to the department.



SIPHOKAZI NDUDANE (Ms)

HEAD OF DEPARTMENT: DRDAR

DATE: 29/05/23

1. INTRODUCTION

Risk management is an area that is constantly changing to fit in line with changes in the business environment. Traditionally, the focus of risk has always been on the management of financial risks in organisations. This is no longer the case; the approach is broadened beyond financial risk management. The area of risk management is intensely regulated in the public service with various statutory obligations regarding processes and control measures, as well as standards.

The risk management policy considers the following additional broad areas of risk:

- a) Strategy
- b) People
- c) Technology
- d) Processes
- e) External environment and natural factors
- f) Legal compliance

This policy details procedures linked to risk management and its processes to minimise the occurrence of risks and ensure proper administrative and management procedures in the Department. It ensures that internal controls are adhered to; improved and implemented by all officials and management of the Department. This policy must be read together with the National Treasury Public Sector Risk Management Framework, Fraud Prevention and Security Management related policies.

Value is created, preserved or eroded by management decisions ranging from strategic planning to daily operations of the department. Inherent in decisions is the recognition of risks, requiring that management consider information about the internal and external environment; deploys precious resources and appropriately adjusts departmental activities to changing circumstances. For governmental institutions, value is realised when constituents recognise receipt of valued services at an acceptable cost. Risk management facilitates management's ability to create both sustainable value and communicate the value created to stakeholders.

The following factors require consideration when integrating ERM into institutional decision making structures:

- a. Aligning risk management with objectives at all levels of the Department;
- b. Introducing risk management components into existing planning and operational practices;
- c. Communicating institutional directions on an acceptable levels of risk;
- d. Including risk management as part of employees' performance appraisals and business unit's annual operations; and
- e. Continuously improving controls and accountability systems and processes to take into account risk management and its results.

2. BACKGROUND

The department is bound by its constitutional mandate to provide services or goods in the interests of the public good. The public sector environment is fraught with unique challenges such as inadequate capacity, excessive bureaucracy and silo mentality, limited resources, competing priorities and infrastructure backlogs to mention a few. Risk management is a management tool which increases the department's prospects of success through minimising negative outcomes and optimising opportunities. Local and international trends confirm that risk management is a strategic imperative rather than an option within high performance organisations. High performing organisations set clear and realistic objectives, develop appropriate strategies aligned to the objectives, understand the intrinsic risks associated therewith and direct resources towards managing such risks on the basis of cost-benefit principles. The department must, in accordance with the prescripts mentioned below, implement and maintain effective, efficient and transparent systems of risk management and internal control therefore ensuring that through its risk management processes it achieves, amongst others, the following outcomes needed to underpin and enhance performance:

- a) More sustainable and reliable delivery of services;
- b) Informed decisions underpinned by appropriate rigour and analysis;
- c) Innovation;
- d) Reduced waste;
- e) Prevention of fraud and corruption;
- f) Better value for money through more efficient use of resources; and
- g) Better outputs and outcomes through improved project and programme management.

3. REGULATORY FRAMEWORK

3.1 CONSTITUTIONAL MANDATE

The mandate of the Department is derived from section 27(1) (b) and 2 of the Constitution of South Africa, 1996, that is,

“..take reasonable legislative and other measures, within its available resources, to achieve the progressive realization of the ... right (of everyone) to have access to sufficient food”

3.2 PFMA AND TREASURY REGULATIONS

3.2.1 PFMA: Section 38(1)(a)(i) states that the accounting officer of a department, must ensure that the department, has and maintains **effective, efficient and transparent systems** of financial and **risk management** and **internal control**

3.2.2 Treasury Regulations: Paragraph 3.2.1 states that the accounting officer must ensure that:

- 3.2.2.1 **Risk assessment is conducted regularly to identify emerging risks** of the department;
- 3.2.2.2 A **risk management strategy**, which must include a, must be used to direct internal audit efforts and priority, and to determine the skills required of managers and staff to improve controls and to manage these risks.
- 3.2.2.3 The strategy must be **clearly communicated to all officials** to ensure that the risk management strategy is **incorporated into the language and culture** of the Department

3.3 ADDITIONAL LEGISLATION

The legislative mandates are informed by the following Acts

1. The Agriculture Development Act, 1999 (Act No. 67 of 1995)
2. Conservation of Agricultural Resources Act, 1983 (Act No. 43 of 1983)
3. The Eastern Cape Rural Finance Corporation Act, 1999 (Act No. 9 of 1999 as amended by Act No. 1 of 2012)
4. Veterinary and Para-Veterinary Professions Act, 1982 (Act No. 19 of 1982)
5. The Animal Health Act, 2002 (Act No. 7 of 2002)
6. The Animal Identification Act, 2002 (Act No. 6 of 2002)
7. The Meat Safety Act, 2000 (Act No. 40 of 2000)
8. Animal Disease Act, 1984 (Act No. 35 of 1984)
9. Animal Improvement Act, 1998 (Act No. 62 of 1998)
10. Animal Protection Act, 1962 (Act No. 71 of 1962)
11. Livestock Improvement Act, 1997 (Act No. 25 of 1997)
12. Agricultural Pests Act, 1983 (Act No. 36 of 1983)
13. Fertilizers, Farm Feeds, Agricultural Remedies and Stock Remedies Act, 1947 (Act No. 36 of 1947)
14. Agricultural Research Amendment Act, 2001 (Act No. 27 of 2001)
15. Marketing of Agricultural Products Act, 1996 (Act No. 47 of 1996)
16. Fencing Act, 1963 (Act No. 31 of 1963)
17. Land Tenure Rights Act, 1991 (Act No. 112 of 1991)
18. Intergovernmental Relations Framework Act, 2005 (Act No. 13 of 2005)
19. Basic Conditions of Employment Act, 1997 (Act No. 75 of 1997)
20. Division of Revenue Act, 2009 (Act No. 12 of 2009)
21. Preferential Procurement Policy Framework Act, 2000 (Act No. 5 of 2000)
22. Public Service Act and Regulations, 1994 (Act No. 103 of 1994)
23. Skills Development Act, 1998 (Act No. 97 of 1998)
24. Occupational Health and Safety Act, 1993 (Act No. 85 of 1993)
25. Employment Equity Act, 1998 (Act No. 55 of 1998)
26. Promotion of Access to Information Act, 2000 (Act No. 2 of 2000)
27. Promotion of Administrative Justice Act, 2000 (Act No. 2 of 2000)

3.4 BEST PRACTICES

King IV Report on Corporate Governance states that risk management is an **integral part of strategic and operational activities**. **Good corporate governance** requires

that **risks to an organisation** must be **properly identified, evaluated** and **mitigated**. Systems and processes should be in place for designing, implementing and monitoring the process of risk management and integrating it into the day to day activities of an organisation.

4. OBJECTIVES

To ensure that:

- 4.1 Financial, operational and management systems directly support the management of risks that threaten the achievement of the department's objectives;
- 4.2 Management have an active, structured and commonly shared knowledge of the whole range and the relative priority of risks that have to be managed;
- 4.3 Managers at every level must share the understanding of risks and priorities;
- 4.4 Responsibility for the management of risks is assigned to staff that have the authority to ensure that they are managed;
- 4.5 Resources are allocated to the management of risks in such a way that optimum value for money is achieved;
- 4.6 Management priorities in respect of risks are fully communicated down the organisation;
- 4.7 Management's view must be informed by upward reporting of risks through the organisation; and
- 4.8 The risk management system should function efficiently; and effectively integrates with the department's planning processes.

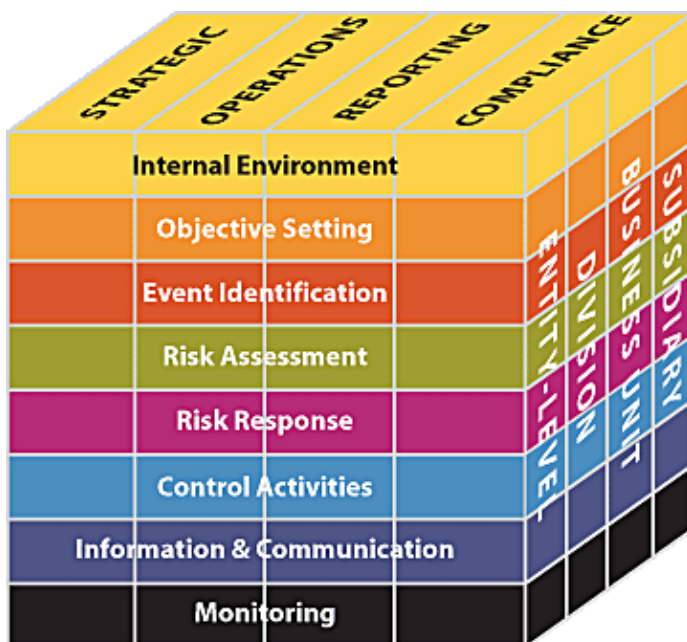
5. OWNERSHIP OF RISK MANAGEMENT

- 5.1 The responsibility for ensuring risk management processes vests in the Accounting Officer.
- 5.2 The Accounting Officer is the primary custodian of risk management in the Department.
- 5.3 The Risk Management office must be established as a support function to ensure the effective management of risks in the Department.
- 5.4 In order to assist in the general facilitation and coordination of risk management processes (as well as the necessary analysis and development of standards), the Accounting Officer must establish the Risk Management Unit headed by a Chief Risk Officer.
- 5.5 This function is of strategic importance and is delegated to the various tiers of management (and supervision) in order to ensure that the risk management function is performed throughout the Department.

6. APPROACH: PROCESS FRAMEWORK

- a. The Department must adopt an entity-wide approach to risk management and is required to view its risk from a portfolio or departmental (entity) wide perspective.
- b. The Enterprise wide risk management (ERM) approach is a dynamic process that consists of eight interrelated components that must permeate every aspect of the Department.
- c. It is expected that ERM processes must become embedded into all key aspects of the Department including its activities, systems, process, and operations.
- d. Furthermore, management must ensure compliance with relevant legislation as the Department endeavours to fulfil the expectations of employees and other stakeholders.

Source: COSO ERM Framework



6.1 CREATING AN ENABLING/INTERNAL ENVIRONMENT / INTERNAL ENVIRONMENT

6.1.1 CREATING AN ENABLING ENVIRONMENT FOR THE MANAGEMENT OF RISKS

- 6.1.1.1 The Accounting Officer must ensure that the institutional environment (Internal Environment) supports the effective functioning of risk management;
- 6.1.1.2 The Department's internal environment is the foundation of risk management, providing the underpinning culture, discipline and structures that influence how strategy and objectives are established, how departmental activities are planned and executed and how risks are identified, assessed and acted upon;
- 6.1.1.3 To give effect to 6.1.1.1 above the Accounting Officer must ensure that the Department:

- 6.1.1.3.1 Operates within its constitutional mandate;
- 6.1.1.3.2 Adopts a value system founded on a public service ethos;
- 6.1.1.3.3 Possesses the inherent competencies required to execute its mandate;
- 6.1.1.3.4 Adopts management practices that embrace the concepts of delegation of authority, personal responsibility, accountability and performance management; and
- 6.1.1.3.5 Has an appropriate organisational structure supported by basic financial and management systems underpinned by risk management and internal controls.

6.1.2 RISK MANAGEMENT POLICY

- 6.1.2.1 The department must operate within the terms of the terms of the approved Risk Management Framework and Policy; and
- 6.1.2.2 The policy must be communicated to all incumbent officials and arrangements must be made for communicating the policy to all new recruits.

6.1.3 RISK MANAGEMENT STRATEGY

- 6.1.3.1 The implementation of this policy must be guided by a strategy approved by the Accounting Officer;
- 6.1.3.2 The Strategy must include:
 - 6.1.3.2.1 A plan of action to improve the department's risk management maturity;
 - 6.1.3.2.2 The department's risk management architecture and reporting lines;
 - 6.1.3.2.3 Details of review and assurance of the risk management process.

6.1.4 ORGANISATIONAL STRUCTURE

- 6.1.4.1 The Accounting Officer must delegate roles and responsibilities in a manner that ensures effective co-ordination and synergy of risk management activities.
- 6.1.4.2 To give effect to 6.1.2.1 above, the business units, working groups and committees must be structured and coordinated in a way that provides a complete perspective of the department's risk exposures and opportunities.

6.1.5 HUMAN RESOURCE CAPACITY

- 6.1.5.1 Adequate human resources capacity, represented by the requisite number of people with the right skills, is fundamental to implement the right risk management strategy.
- 6.1.5.2 Internal processes must be established to sensitise all employees of the relevance of risk management to the achievement of their performance goals.
- 6.1.5.3 Training and support must be provided to everyone involved in risk management activities to equip them to optimally execute their responsibilities for risk management as set out under Roles and Responsibilities.

6.1.5.4 The Chief Risk Officer and his/her staff must possess the necessary skills, competencies and attitudes to execute the functions set out under roles and responsibilities.

6.1.6 TOOLS AND TECHNOLOGY

6.1.6.1 Tools and technology can produce considerable efficiencies by simplifying complex processes and accelerating otherwise time consuming tasks in the risk management process.

6.1.6.2 Where appropriate consideration must be given to the use of automated tools for capturing, organising, storing and interrogating data, as well as communicating and tracking information.

6.1.6.3 Notwithstanding 6.1.4.1 and 6.1.4.2 above, all officials must be mindful of the fact that technology is not a substitute for the human endeavour and intellect required for effective risk management,

6.1.7 FUNDING RISK MANAGEMENT ACTIVITIES

6.1.7.1 Funding is required to cover the cost of implementing, maintaining and continuously improving the state of risk management and control.

6.1.7.2 The Chief Risk Officer must control operating and capital costs of the Risk Management Unit.

6.1.7.3 The cost of implementing and improving controls must be the responsibility of Risk Owners, who must provide for such costs in their capital or operational budgets as the case may be.

6.1.7.4 Investment in risk management and control must be considered on the basis of cost versus benefit.

6.2 OBJECTIVE SETTING

6.2.1 The Accounting Officer must establish objectives that are consistent with the Department's constitutional mandate and ensure that its services are appropriate, economical, efficient and equitable;

6.2.2 The Accounting Officer must ensure that:

6.2.2.1 Objectives are finalised through a rigorous analysis of the costs and benefits associated therewith;

6.2.2.2 The Department has and maintains an effective process to identify the risks inherent in the chosen objectives; and

6.2.2.3 The Department is able to manage such risks effectively, economically and efficiently.

6.3 EVENT IDENTIFICATION

6.3.1 Risk identification is a deliberate and systematic effort to identify and document the department's key risks;

6.3.2 The objective of risk identification is to understand what is at risk within the context of the department's explicit and implicit objectives and to generate a

- comprehensive inventory of risks based on the threats and events that might prevent, degrade, delay or enhance the achievement of the objectives;
- 6.3.3 The department must adopt a rigorous and ongoing process of risk identification that also include mechanisms to timely identify new and emerging risks;
 - 6.3.4 The risk identification process must cover all risks, regardless of whether or not such risks are within the direct control of the department;
 - 6.3.5 Risk identification must be inclusive, not overly rely on the inputs of a few senior officials and must also draw as much as possible on unbiased independent sources, including the perspectives of important stakeholders;
 - 6.3.6 Risk workshops and interviews are useful for identifying, filtering and screening risks but it is important that these judgement based techniques be supplemented by more robust and sophisticated methods where possible, including quantitative techniques;
 - 6.3.7 Risk identification must be strengthened by supplementing management's perceptions of risks. Inter alia, with:
 - 6.3.7.1 Review of external and internal audit reports;
 - 6.3.7.2 Review of the reports of the Standing Committee on Public Accounts and the relevant Parliamentary or Legislature Committee(s);
 - 6.3.7.3 Financial analyses;
 - 6.3.7.4 Historic data analyses;
 - 6.3.7.5 Actual loss data;
 - 6.3.7.6 Interrogation of trends in key performance indicators;
 - 6.3.7.7 Benchmarking against peer group or quasi peer group;
 - 6.3.7.8 Market and sector information;
 - 6.3.7.9 Scenario analyses; and
 - 6.3.7.10 Forecasting.
 - 6.3.8 To ensure comprehensiveness of risk identification the department must identify risk factors through considering both external and internal factors, through appropriate processes of:
 - 6.3.8.1 Strategic risk Identification to identify risks emanating from the strategic choices made by the department, specifically with regard to whether such choices weaken or strengthen the department's ability to execute its constitutional mandate;
 - 6.3.8.2 Strategic risk identification must precede the finalisation of strategic choices to ensure that potential risk issues are factored into the decision making process for selecting strategic options;
 - 6.3.8.3 Risks inherent to the selected strategic choices must be documented, assessed and managed through the normal functioning of the system of risk management; and
 - 6.3.8.4 Strategic risks must be formally reviewed concurrently with changes in strategy, or at least once a year to consider new and emerging risks.
 - 6.3.9 Operational risk identification to identify risks concerned with the department's operations:
 - 6.3.9.1 Operational risk identification must seek to establish vulnerabilities introduced by employees, internal processes and systems, contractors, regulatory authorities and external events;

- 6.3.9.2 Must be an embedded continuous process to identify new and emerging risks and consider shifts in known risks through mechanisms such as environmental scanning, process reviews and the like; and
- 6.3.9.3 To the extent that 6.3.9.2 above is deemed adequate to expose the full extent of risk introduced by significant environmental or institutional changes, operational risk identification must be repeated when changes occur, or at least once a year, to identify emerging risks.
- 6.3.10 Project risk identification to identify risks inherent to particular projects:
 - 6.3.10.1 Project risks must be identified for all major projects, covering the whole lifecycle; and
 - 6.3.10.2 For long term projects, the project risk register must be reviewed at least once a year to identify new and emerging risks.

6.4 RISK ASSESSMENT

- 6.4.1 Risk assessment is a systematic process to quantify or qualify the level of risk associated with a specific threat or event, to enrich the risk intelligence available to the department.
- 6.4.2 The main purpose of risk assessment is to help the department to prioritise the most important risks as it does not have the capacity to deal with all risks in an equal manner.
- 6.4.3 Risks must be assessed on the basis of the likelihood of the risk occurring and the impact of its occurrence on the particular departmental objective/s it is likely to affect.
- 6.4.4 Risks must be expressed in the same unit of measure used for the key performance indicators/s concerned.
- 6.4.5 Risk assessment must be performed through a three stage process:
 - 6.4.5.1 Firstly, the inherent risk must be assessed to establish the level of exposure in the absence of deliberate management actions to influence the risk (current controls);
 - 6.4.5.2 Secondly, a residual risk assessment must follow the process described in 6.4.5.1 above to determine the actual remaining level of the risk after the mitigating effects of management actions to influence risk or application of current controls; and
 - 6.4.5.3 Thirdly, the residual risk must be benchmarked against the department's risk appetite to determine the need for further management intervention, if any.
- 6.4.6 Risk assessment must be strengthened where possible by supplementing management's perceptions with the methods referred to 6.3.7 above.
- 6.4.7 Risk assessment must be re-performed for the key risks in response to significant environmental and/or organisational changes, but at least once a year, to ascertain the shift in the magnitude of risk and the need for further management action as a result thereof.

6.5 RISK RESPONSE

- 6.5.1 Risk response is concerned with developing strategies to reduce or eliminate the threats and events that create risks.
- 6.5.2 Risk response must also make provision for the exploitation of opportunities to improve the performance of the department.
- 6.5.3 Responding to risk involves identifying and evaluating the range of possible options to mitigate risks and implementing the chosen option.
- 6.5.4 Management must develop response strategies for all material risks, whether or not the management thereof is within the direct control of the department, prioritising the risks exceeding or nearing the risk appetite level.
- 6.5.5 When the management of the risk is within the control of the department, the response strategies must consider:
 - 6.5.5.1 Avoiding the risk, for example, choosing a different strategy or terminating the activity that produces the risk;
 - 6.5.5.2 Treating the risk by, for example, implementing or improving the internal control system;
 - 6.5.5.3 Transferring the risk to another party more competent to manage it by, for example, contracting out services, establishing strategic partnerships and buying insurance;
 - 6.5.5.4 Accepting the risk where cost and strategy considerations rule out alternatives strategies; and
 - 6.5.5.5 Exploiting the risk factors by implementing strategies to take advantage of the opportunities presented by such risk factors.
- 6.5.6 In instances where the management of the risk is not within the control of the department the response strategies must consider measures such as forward planning and lobbying.
- 6.5.7 Response strategies must be documented and the responsibilities and timelines attached thereto must be communicated to the relevant persons.

6.6 CONTROL ACTIVITIES: DESIGNING CONTROL ACTIVITIES TO MITIGATE RISKS

- 6.6.1 Management is responsible for designing, implementing and monitoring the effective functioning of systems of internal controls
- 6.6.2 Without derogating from the above, everyone in the department must also have responsibilities for maintain effective systems of internal controls consistent with their delegated authority.
- 6.6.3 Management must develop the internal control architecture through:
 - 6.6.3.1 **Preventative controls:** To prevent errors or irregularities from occurring, e.g. physical security of assets to prevent theft;
 - 6.6.3.2 **Detective Controls:** To find errors or irregularities after they have occurred, e.g. performance of reconciliation procedures to identify errors;

- 6.6.3.3 **Corrective Controls:** That operate together with detective controls to correct errors or irregularities.
- 6.6.4 The internal control architecture must include:
 - 6.6.4.1 **Management controls** to ensure that the department's structure and systems support its policies, plans and objectives, and that it operates within laws and regulations;
 - 6.6.4.2 **Administrative controls** to ensure that policies and objectives are implemented in an effective and efficient manner;
 - 6.6.4.3 **Accounting controls** to ensure that resources are accounted for fully and transparently and are properly documented; and
 - 6.6.4.4 **Information technology controls** to ensure security, integrity and availability of information.

6.7 COMMUNICATION AND REPORTING

- 6.7.1 Relevant information, properly and timely communicated is essential to equip the relevant officials to identify, assess and respond to risks.
- 6.7.2 The department's risk communication and reporting process must support enhanced decision making and accountability through:
 - 6.7.2.1 Communication of relevant, timely, accurate and complete information; and
 - 6.7.2.2 Communicating responsibilities and actions.

6.8 MONITORING

- 6.8.1 Monitoring concerns checking on a regular basis to confirm the proper functioning of the entire risk management system.
- 6.8.2 Monitoring must be effected through ongoing activities or separate evaluations to ascertain whether risk management is effectively practised at all levels and across the department in accordance with the Policy, Strategy and Implementation Plan.
- 6.8.3 Monitoring activities must focus on evaluating whether:
 - 6.8.3.1 Allocated responsibilities are being executed effectively;
 - 6.8.3.2 Response strategies are producing the desired result of mitigating risks or exploiting opportunities; and
 - 6.8.3.3 A positive correlation exists between improvements in the system of risk management and departmental performance.

7 RISK APPETITE AND RISK TOLERANCE

Risk Appetite and Risk Tolerance would be outlined in a separate framework which would indicate acceptable and unacceptable risks. Risk appetite is the amount and

type of risks the department is prepared to accept and for which it has the unique competency to manage, or know that the department can neither manage nor mitigate, in order to meet its objectives. The department's statement on risk appetite and tolerance is intended to guide employees in their actions and to direct decisions regarding the acceptability of specific risks.

8 INTEGRATION OF RISK MANAGEMENT ACTIVITIES

- 8.1 ERM is a broad-based application of risk management in all major functions and activities of the department, rather than in selected areas, to isolate the material risks.
- 8.2 It represents a response to the dilemma that risks (including opportunities) are dynamic and often highly interdependent and need to be managed through a portfolio approach rather than as separate and static events, to achieve comprehensive and integrated attention.
- 8.3 It also calls on the department to look beyond itself, requiring the consideration of risks on performance regardless of whether the risk is internally or externally generated.
- 8.4 To give effect to 8.3 above, the department must:
 - 8.4.1 Communicate timely with other organs of state in instances where the identification, evaluation and management of risk to the department require the participation of these organs;
 - 8.4.2 Identify and communicate to other organs of state risks posed to them by the department's own actions or inaction; and
 - 8.4.3 Consider the material risks throughout the value chain responsible for producing and delivering particular services or goods, to appreciate the threats posed by the non-performance of the parties in the value chain.
- 8.5 The department must be aware of and comply with various legislation that prescribe the specific treatment of risk within their ambit, for example, Occupational Health and Safety Act, Disaster Management Act and others.
- 8.6 Formal channels of communication and cooperation must exist within the department to facilitate synergy between the Risk Management Unit and Risk Management Committee, and internal formations concerned with risk mitigation, including but not limited to formations responsible for:
 - 8.6.1 Occupational health and safety;
 - 8.6.2 Business continuity management;
 - 8.6.3 Prevention of fraud and corruption; and
 - 8.6.4 Awarding of bids/tenders.

9 SCOPE OF THE POLICY

The policy is applicable to all employees of and stakeholders contracted by the Department of Rural Development and Agrarian Reform.

10 IMPLEMENTATION PROCEDURES: RISK MANAGEMENT STRATEGY AND IMPLEMENTATION PLAN

- 10.1. The implementation procedures outlined in this policy must be read in conjunction with the Risk Management Strategy and Implementation Plan.
- 10.2. The Enterprise Risk Management Policy must be implemented in terms of the Risk Management Strategy and Risk Management Implementation Plan approved by the Accounting Officer.
- 10.3. Both the Strategy and Implementation Plan must be reviewed on an annual basis, to ensure that they are in line with new developments in risk management and changes to the departmental strategic focus.
- 10.4. The aforementioned documents must serve as the procedure manual of the policy.

11 ROLES, RESPONSIBILITIES AND GOVERNANCE

Below are some of the functions of the stakeholders of risk management extracted from the **Public Sector Risk Management Framework** issued by **National Treasury**. Refer to the abovementioned framework for other functions as the ones listed below are not the only ones.

11.1 EXECUTIVE AUTHORITY

- 11.1.1. The Executive Authority takes interest in risk management to the extent necessary to obtain comfort that properly established and functioning systems are in place.
- 11.1.2. High level responsibilities must include:
 - 11.1.2.1. Ensuring that the departmental strategies are aligned to its mandate;
 - 11.1.2.2. Obtaining assurance from management that the department's strategic choices were based on a rigorous assessment of risk;
 - 11.1.2.3. Obtaining assurance that key risks inherent in the department's strategies were identified and assessed, and are being properly managed;
 - 11.1.2.4. Assisting the Accounting Officer to deal with fiscal, intergovernmental, political and other risks beyond their direct control and influence;
 - 11.1.2.5. Insist on the achievement of objectives, effective performance management and value for money

11.2 ACCOUNTING OFFICER

- 11.2.1. The Accounting Officer is the ultimate Chief Risk Officer and is accountable for the department's governance of risk;
- 11.2.2. High level (and not all) responsibilities include:
 - 11.2.2.1. Setting an appropriate tone by supporting and being seen to be supporting the department's aspiration for effective risk management;
 - 11.2.2.2. Delegating responsibilities for risk management to management and formation of internal structures such as Risk Management Committee and other governance committees;
- 11.2.3. Holding management accountable for designing, implementing, monitoring and integrating risk management into their day-to-day activities.
- 11.2.4. Holding the internal structures accountable for performance in terms of their responsibilities for risk management;
- 11.2.5. Providing leadership and guidance to enable management and internal structures responsible for various aspects of risk management to properly perform their functions;
- 11.2.6. Ensuring that the control environment supports the effective functioning of risk management as discussed in paragraph 6.1 above;
- 11.2.7. Approving the Risk Management Policy, Risk Management Strategy and Implementation Plan;
- 11.2.8. Approving the Department's risk appetite and risk tolerance;
- 11.2.9. Devoting personal attention to overseeing management of significant risks;
- 11.2.10. Leveraging the Audit Committee, Internal Audit, External Audit and Risk Management Committee for assurance of risk management;
- 11.2.11. Ensuring appropriate action in respect of the recommendations of the Audit Committee, Internal Audit, External Audit and Risk Management Committee to improve risk management;
- 11.2.12. Providing assurance to relevant stakeholders that key risks are properly identified, assessed and mitigated.

11.3 AUDIT COMMITTEE

- 11.3.1 The responsibilities of the Audit Committee with respect to risk management shall be formally defined in its Charter.
- 11.3.2 The Audit Committee is responsible for oversight of the department's control, governance and risk management.
- 11.3.3 Furthermore the Audit Committee shall provide the Accounting Officer with independent counsel, advice and direction in respect of risk management.
- 11.3.4 The Audit Committee must provide an independent objective view of the effectiveness of Department's risk management;
- 11.3.5 The responsibilities of the Audit Committee include ensuring the Internal Audit and External Audit Plans are aligned to the Risk Profile of the Department;
- 11.3.6 Satisfy itself that it has appropriately addressed the following areas:
 - 11.3.6.1 Financial reporting risks, including the risk of fraud;

- 11.3.6.2 Internal financial controls; and
- 11.3.6.3 IT risks as they relate to financial reporting.
- 11.3.7 Evaluate the effectiveness of Internal Audit in its responsibilities for risk management.

11.4 INTERNAL AUDIT

The responsibilities of Internal Audit are formally outlined in the Internal Audit Charter. Listed below are some of the responsibilities of Internal Audit:

- 11.4.1. The role of the Internal Auditing in risk management is to provide an independent, objective assurance on the effectiveness of the department's system of risk management;
- 11.4.2. Evaluate the effectiveness of the entire system of risk management and provide recommendations for improvement where necessary;
- 11.4.3. Develop its internal audit plan on the basis of the key risk areas;
- 11.4.4. In terms of the International Standards for the Professional Practice of Internal Audit, determining whether risk management processes are effective is a judgment resulting from the Internal Auditor's assessment that:
 - 11.4.4.1. Institutional objectives support and align with the Institution's mission;
 - 11.4.4.2. Significant risks are identified and assessed;
 - 11.4.4.3. Risk responses are appropriate to limit risk to an acceptable level; and
 - 11.4.4.4. Relevant risk information is captured and communicated in a timely manner to enable the Accounting Officer, Management, the Risk Management Committee and other officials to carry out their responsibilities.

11.5 RISK MANAGEMENT COMMITTEE

- 11.5.1. The Risk Management Committee must be appointed by the Accounting Officer to assist him to discharge his responsibilities for risk management.
- 11.5.2. The Accounting Officer must appoint an independent Chairperson for the Risk Management Committee;
- 11.5.3. The responsibilities of the Committee and Chairperson must be formerly outlined in its charter.

11.6 CHIEF RISK OFFICER

- 11.6.1 The primary responsibility of the Chief Risk Officer is assist the department to embed risk management and leverage its benefits to enhance performance;
- 11.6.2 As head of the Risk Management Unit the CRO is the custodian of the ERM Strategy with a mandate to coordinate all risk management activities throughout DRDAR;

- 11.6.3 Tasked with the overall efficiency of the ERM function as well as embedding risk management practices and fostering a risk aware culture within the department, the CRO assists in integrating risk management throughout the department;
- 11.6.4 Working with senior management to develop the department's vision for risk management;
- 11.6.5 Developing, in consultation with management, the department's risk management framework incorporating inter alia:
 - 11.6.5.1 Risk Management Policy;
 - 11.6.5.2 Risk Management Strategy;
 - 11.6.5.3 Risk Management Implementation Plan;
 - 11.6.5.4 Risk identification and assessment methodology;
 - 11.6.5.5 Risk appetite and tolerance
- 11.6.6 Communicating the department's risk management framework and Strategy to all stakeholders in the department and monitoring its implementation;
- 11.6.7 Facilitating orientation and training for the Risk Management Committee;
- 11.6.8 Training all stakeholders in their risk management functions;
- 11.6.9 Continuously driving risk management to higher levels of maturity;
- 11.6.10 Assisting management with risk identification, risk assessment and response strategies;
- 11.6.11 Monitor the implementation of the risk response strategies;
- 11.6.12 Collating, aggregating, interpreting and analysing the results of risk assessments to extract risk intelligence;
- 11.6.13 Reporting risk intelligence to the Accounting Officer, management and the Risk Management Committee; and
- 11.6.14 Participating with Internal Audit, Management, and Auditor General in developing the combined assurance plan for the department.
- 11.6.15 Provide risk advice on all operations of the Department.

11.7 MANAGEMENT

- 11.7.1 Management is responsible for executing their responsibilities outlined in the Risk Management Strategy and Implementation Plan and for integrating risk management into the operational routines.
- 11.7.2 Empowering officials to perform effectively in their risk management responsibilities through proper communication of responsibilities, comprehensive orientation and ongoing opportunities for skills development;
- 11.7.3 Aligning the functional risk management methodologies and processes and departmental processes;
- 11.7.4 Devoting personal attention to overseeing the management of key risks within their area of responsibility;
- 11.7.5 Maintaining a cooperative relationship with the Chief Risk Officer, Risk Management Unit, Risk Owners and Risk Champions;

- 11.7.6 With the help of the Risk Management Unit – identify risks within their line function;
- 11.7.7 Designing and implementing controls to mitigate identified risks;
- 11.7.8 Analyse controls for adequacy and effectiveness and implement corrective and improvement measures;
- 11.7.9 Maintaining the proper functioning of the internal control processes within their area of responsibility;
- 11.7.10 Monitoring risk management within their area of responsibility;
- 11.7.11 Implementing the directives of the Accounting Officer concerning risk management;
- 11.7.12 Providing risk management reports and presentations to the Risk Management Committee and Audit Committee as requested; and
- 11.7.13 Holding employees accountable for their specific risk management responsibilities.

11.8 RISK OWNERS

- 11.8.1 Risk Owners are those officials responsible for controlling (fully or partly) one of the significant risks.
- 11.8.2 Risk Owners must be appointed by the Accounting Officer, and their responsibility amongst others, is to identify Action Plans/Risk Treatment Plans for identified risks, detailing what actions will be taken to address the risks including preventative measures, disaster recovery and business continuity plans.
- 11.8.3 Reports and portfolio of evidence for all risks within their responsibility would collated regularly (quarterly) and submitted to the CRO for review and comment.
- 11.8.4 Key Risk Indicators (KRIs) for each risk will be identified as part of Risk Treatment Planning and the CRO will provide the necessary support required by Risk Owners to report on each risk within their responsibility.

11.9 OTHER EMPLOYEES

- 11.9.1 Other officials are accountable to their managers for implementing and monitoring the process of risk management and integrating it into their day-to-day activities;
- 11.9.2 Other officials are accountable to their managers for implementing and monitoring the process of risk management and integrating it into their day-to-day activities.
- 11.9.3 Applying risk management processes in their respective functions;
- 11.9.4 Implementing the delegated action plans to address identified risks;
- 11.9.5 Inform their supervisors and/or Risk Management Unit of new risks and significant changes in known risks;

- 11.9.6 Cooperate with other role players in the risk management process and provide information as required;
- 11.9.7 Adhering to the code of conduct and code of ethics of the public service;
- 11.9.8 Maintaining the functioning of internal control processes, information and communication as well as the monitoring systems within their area of responsibility;
- 11.9.9 Participating in risk identification and risk assessment processes within their business unit;
- 11.9.10 Reporting inefficient, unnecessary and unworkable controls; and
- 11.9.11 Reporting suspicion of fraud and corruption to the Anti-corruption unit through the whistleblowing processes.

11.10 RISK CHAMPIONS

- 11.10.1 A Risk Champion is a person with the skills, knowledge and power of office required to champion a particular aspect of risk management. A key part of the Risk Champions' responsibility involves facilitating implementation of risk management principles in their areas of responsibility.
- 11.10.2 The Risk Champion also adds value to the risk management process by providing support to the CRO in terms of information requirements and reports.
- 11.10.3 A Risk Champion shall act as change agents in the risk management process and ensure that risk treatment plans are implemented within their area of responsibility and report on progress;
- 11.10.4 The Risk Champion must not assume the role of Risk Owner but should assist the Risk Owner to resolve problems.

11.11 EXTERNAL AUDIT

Chairperson to assist:

- 11.11.1 The responsibilities of Auditor General (AG) are outlined in the Public Audit Act. As external auditors the AG is required to perform an audit of the department's activities on an annual basis or whenever it is required and prepare a report on the audit reflecting their independent opinion and statements on:
 - 11.11.1.1 Whether the annual financial statements of DRDAR fairly present in all material respects, the financial position at a specific date and results of the department's operations and cash flow for the period under review;
 - 11.11.1.2 DRDAR's compliance with any applicable legislation relating to financial matters, financial management and other related matters; and
 - 11.11.1.3 The reported information relating to the performance of the department against predetermined objectives.

12 COMPILATION AND MAINTENANCE OF RISK REGISTERS

- 12.1. Risk Management Unit must facilitate the risk identification and risk assessment process for all programs of the Department.
- 12.2. Management must at the same time identify current controls and action plans to improve the management of risks.
- 12.3. The risk register must as a minimum contain the following information:
 - 12.3.1. Strategic objectives;
 - 12.3.2. Risk category;
 - 12.3.3. Risk description;
 - 12.3.4. Root causes of the risk;
 - 12.3.5. Consequences of the risk;
 - 12.3.6. Inherent risk rating with its ratings of likelihood and impact;
 - 12.3.7. Current Internal Controls (including whether it is a preventative, detective or corrective control);
 - 12.3.8. Residual risk rating based on the perceived control effectiveness and control adequacy of the current controls;
 - 12.3.9. Identify key risk indicators;
 - 12.3.10. Identify actions plans to improve management of risks with due dates; and
 - 12.3.11. Identify – Risk Owners and Risk Champions.
- 12.4. The process of risk assessment must be finalised before the start of a new financial year.
- 12.5. The Risk Register of the Department must be approved by the Accounting Officer.
- 12.6. Management and other employees of the Department are responsible for the maintenance of the risk register.

13 RESOURCE IMPLICATIONS

The implementation and management of this policy require provision of human and financial resources by DRDAR as follows:-

- 13.1 Through provision of human and financial resources for Risk Management Unit for the implementation and management of the policy;
- 13.2 Establishment of a Risk Management Committee with an external independent Chairperson;
- 13.3 Programme Managers are responsible for budgeting for the implementation of the policy within the programmes by ensuring adequate resources are set aside for mitigation of identified risks.

14 RISK MANAGEMENT MATURITY

- 14.1. There are five different levels of risk management maturity, viz:
 - 14.1.1. Level 1: Non-existent
 - 14.1.2. Level 2: Initial/Ad Hoc
 - 14.1.3. Level 3: Repeatable

- 14.1.4. Level 4: Managed
- 14.1.5. Level 5: Optimized

14.2. The department must in addition to other provisions in the policy ensure that the following activities are applied to be able to achieve and maintain the optimized level (Level 5):

- 14.2.1. Use audit and review techniques to keep application of risk management techniques at the required quality and standards;
- 14.2.2. Continually invest in improving the risk process, tools, techniques, technology, personnel skills, etc.;
- 14.2.3. Depending on available resources – fully exploit and integrate technology in all aspects of risk management;
- 14.2.4. Benchmark against other public institutions or even private sector institutions on the level 5 maturity;
- 14.2.5. Implement a programme of continuous improvement, and/or refinement of risk management processes; and
- 14.2.6. Learn from previous experiences, and strive for excellence.

15 REPORTING

Management must submit risk management reports, using the Risk Management Reporting Template to the Chief Risk Officer on a quarterly bases or as determined by the Risk Management Unit. The reports from the Risk Owners must entail progress on the implementation of action plans and on the consolidation of portfolios of evidence in relation to the action plans. The Chief Risk Officer must submit quarterly reports to the Risk Management Committee. The Chairperson of the Risk Management Committee must submit reports to the Audit Committee at each sitting. Quarterly reports must be submitted to the Accounting Officer.

16 EVALUATION OF RISK MANAGEMENT EFFECTIVENESS

16.1 EVALUATION OF VALUE ADD

- 16.1.1 Evaluation of risk management effectiveness is vital to maximise the value created through risk management practices.
- 16.1.2 The department must strive to incrementally and sustainably achieve a mature risk management regime in order to realise the outcomes referred to in section (a) to (g) under the **Background** above.
- 16.1.3 The department must periodically evaluate the value add of risk management by measuring outcomes against preset key performance indicators aligned to the overall goals and objectives of the department.
- 16.1.4 The department must utilise the Financial Management Capability Maturity Model (FMCMM) and other tools developed by National Treasury to evaluate its current and progressive risk management maturity.

16.2 PERFORMANCE INDICATORS

- 16.2.1 Everyone in the department has a part to play in achieving and sustaining a vibrant system of risk management and to that extent must function within a framework of responsibilities and performance indicators.
- 16.2.2 The Accounting Officer must evaluate his own performance in leading the risk management process in the department through the following and other relevant indicators:
 - 16.2.2.1 The risk management maturity trend as measured in terms of an appropriate index such as the Financial Management Capability Maturity Model;
 - 16.2.2.2 The department's performance against key indicators, including comparison of year-on-year performance;
 - 16.2.2.3 The department's "avoided risk" record when compared against the peer group or quasi-peer group;
 - 16.2.2.4 Percentage change in unauthorised, fruitless, wasteful and irregular expenditure based on year-on-year comparisons;
 - 16.2.2.5 Percentage change in incidents and quantum of fraud based on year-on-year comparisons; and
 - 16.2.2.6 Progress in securing improved audit outcomes in regular and performance audits.
- 16.2.3 Insofar as it concerns the responsibilities of the Audit Committee for risk management, the Accounting Officer must evaluate performance of the Committee through the following and other relevant indicators:
 - 16.2.3.1 The Auditor General's management report on the effectiveness of the Audit Committee;
 - 16.2.3.2 The results of the Committee's own 360⁰ assessment;
 - 16.2.3.3 The Committee's co-ordination of the work of Internal Auditing, External Audit and other assurance providers in respect of risk management; and
 - 16.2.3.4 The quality and timeliness of the Audit Committee's counsel and recommendations on matters concerning the system of risk management.
- 16.2.4 The Accounting Officer must evaluate the performance of the Risk Management Committee through the following and other relevant indicators:
 - 16.2.4.1 The result of the Risk Management Committee's own 360⁰ assessment;
 - 16.2.4.2 The pace and implementation of the Risk Management Framework;
 - 16.2.4.3 The Internal Audit report on the state of risk management;
 - 16.2.4.4 The Auditor General's management report on the effectiveness of the Risk Management Committee; and
 - 16.2.4.5 The quality and timeliness of the Risk Management Committee's counsel and recommendations.
- 16.2.5 The Accounting Officer in consultation with the Risk Management Committee, must evaluate the performance of the Chief Risk Officer through the following and other relevant indicators:
 - 16.2.5.1 Developing and implementation of the Risk Management Policy, Strategy and Implementation Plan;

- 16.2.5.2 The department's collective awareness, skill and participation in risk management;
- 16.2.5.3 Risk management maturity;
- 16.2.5.4 Quality and timeliness of support to management, other officials and the Risk Management Committee;
- 16.2.5.5 Quality and timeliness of risk intelligence; and
- 16.2.5.6 Absence of surprises.

16.2.6 The Accounting Officer must evaluate the performance of management through the following and other relevant indicators:

- 16.2.6.1 Business unit performance against key indicators, including comparison of year-on-year performance;
- 16.2.6.2 Implementation of risk management action plans;
- 16.2.6.3 Co-operation with the Risk Management Committee, Risk Champion and relevant stakeholders involved in risk management;
- 16.2.6.4 Quality and timeliness of risk identification, assessment and reporting;
- 16.2.6.5 Proactive identification of new and emerging risks;
- 16.2.6.6 Absence of surprises;
- 16.2.6.7 Year-on-year reduction in adverse incidents and realised losses;
- 16.2.6.8 Elimination of unauthorised, fruitless, wasteful and irregular expenditure;
- 16.2.6.9 Reduction in fraud; and
- 16.2.6.10 Progress in securing improved Internal Audit and Auditor-General outcomes in regularity and performance audits.

16.2.7 The Accounting Officer must evaluate the performance of Risk Champions through the following and other relevant indicators:

- 16.2.7.1 Resolution of delegated problems;

16.2.8 Insofar as it concerns, the responsibilities of Internal Auditing for risk management, the Accounting Officer must evaluate the performance of Internal Auditing through the following and other indicators:

- 16.2.8.1 Timeliness and quality of assurance on risk management;
- 16.2.8.2 Timeliness and quality of recommendations to improve risk management; and
- 16.2.8.3 Adoption of risk based auditing.

16.2.9 Management must evaluate the performance of their staff through the following and other indicators:

- 16.2.9.1 Implementation of risk management action plans.

16.3 MONITORING AND EVALUATION

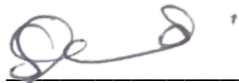
- 16.3.1 If existing controls are weak and exposes the department's activities to risks, management must come up with action plans to reduce risks to an acceptable level.
- 16.3.2 Management must decide on the implementation date of the agreed upon action plan and the responsibility for the implementation of action plan should be assigned to capable officials.

- 16.3.3 It is critical that management must develop key performance indicators regarding the performance of agreed upon controls.
- 16.3.4 Key performance indicators must provide feedback regarding effectiveness of controls against identified risks.
- 16.3.5 Management's performance with the processes of ERM must be measured and monitored through the following performance management activities:
 - 16.3.5.1 Monitoring of progress made by management with the implementation of the ERM methodology;
 - 16.3.5.2 Monitoring of key risk indicators;
 - 16.3.5.3 Monitoring of loss and incident data;
 - 16.3.5.4 Management's progress made with risk mitigation action plans;
 - 16.3.5.5 Annual quality assurance review of ERM performance; and
 - 16.3.5.6 Collecting, analysing and reviewing of portfolio of evidence (POEs) from Risk Owners for each action plan by the set deadline.

17 REVIEW OF POLICY

The ERM Policy will be reviewed over a period of three years. The Chief Risk Officer would conduct research on any new developments and communicate the amendments to the members of the Risk Management Committee prior to the meeting. The Chief Risk Officer would make a representation to the Risk Management Committee for the review to be effected.

18 RECOMMENDATIONS AND APPROVAL OF POLICY



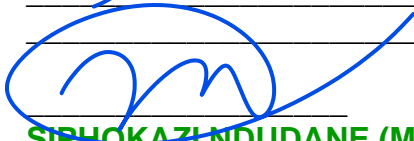
SAMELLA SILI (Ms)
CHIEF RISK OFFICER
DATE: 16 May 2023

Supported/~~Not Supported~~



VUYELWA HLEHLISO
INDEPENDENT CHAIRPERSON: RISK MANAGEMENT COMMITTEE
DATE: 18 May 2023

Approved/Not Approved



SIPHOKAZI NDUDANE (Ms)
HEAD OF DEPARTMENT: DRDAR
DATE: _____