



Province of the

EASTERN CAPE

**RURAL DEVELOPMENT AND
AGRARIAN REFORM**

ENTERPRISE RISK MANAGEMENT STRATEGY AND METHODOLOGY

March 2023

Table Contents

ACRONYMS	iv
DEFINITION OF TERMS AND CONCEPTS	v
LIST OF FIGURES AND TABLES	viii
1. INTRODUCTION	1
2. OBJECTIVE	1
3. APPROACH	1
4. RISK MANAGEMENT MATURITY	1
5. RISK CATEGORIES	2
6. ENTERPRISE RISK MANAGEMENT FRAMEWORK	6
7. RISK MANAGEMENT PROCESS	8
7.1 STEP 1: ESTABLISH THE CONTEXT	10
7.1.1 ESTABLISH STRATEGIC CONTEXT	10
7.1.2 ESTABLISH ORGANISATIONAL CONTEXT	11
7.1.3 ESTABLISH A RISK MANAGEMENT CONTEXT	11
7.1.4 DEVELOP RISK EVALUATION CRITERIA	12
7.2 STEP 2: RISK IDENTIFICATION	14
7.2.1 OBJECTIVE BASED RISK ASSESSMENT MODEL	14
7.2.2 SCENARIO PLANNING	16
7.2.3 ENVIRONMENTAL SCANNING	16
7.2.4 RISK PROFILES	17
7.3 STEP 3: RISK ASSESSMENT	18
7.3.1 RISK ANALYSIS REVIEW	18
7.3.2 RISK EVALUATION	22
7.4 STEP 4: RISK TREATMENT	22
7.4.1 ASSIGNMENT OF RISK OWNERSHIP	22
7.4.2 DETERMINING THE RISK ACCEPTANCE CRITERIA BY IDENTIFYING WHAT RISKS WILL NOT BE TOLERATED	24
7.4.3 DEVELOPMENT OF RISK TREATMENT PLANS	24
7.4.4 IMPLEMENTING RISK TREATMENT PLANS	24
7.5 STEP 5: MONITORING AND REVIEW	25
7.5.1 MONITORING	25
7.5.2 REVIEW	26

7.6	STEP 6: COMMUNICATION AND TRAINING.....	26
7.6.1	COMMUNICATION	27
7.6.2	REPORTING	27
7.6.3	TRAINING	30
8	ROLES, RESPONSIBILITIES AND GOVERNANCE.....	31
8.1	RISK MANAGEMENT IMPLEMENTERS	31
8.1.1	MANAGEMENT	31
8.1.1.1	STRATEGIC VALUE OF MANAGEMENT.....	31
8.1.1.2	RESPONSIBILITIES OF MANAGEMENT	31
8.1.2	OTHER EMPLOYEES	32
8.1.2.1	STRATEGIC VALUE OF OTHER OFFICIALS	32
8.1.2.2	RESPONSIBILITIES FOR OTHER OFFICIALS	32
8.2	RISK MANAGEMENT SUPPORT.....	32
8.2.1	STRATEGIC VALUE OF RISK CHAMPIONS.....	32
8.2.2	RESPONSIBILITIES OF RISK CHAMPIONS	33
8.2.3	RISK OWNERS.....	33
8.2.4	STRATEGIC VALUE OF CHIEF RISK OWNER	33
8.2.5	RESPONSIBILITIES OF THE CHIEF RISK OFFICER	33
8.3	RISK MANAGEMENT ASSURANCE PROVIDERS	34
8.3.1	STRATEGIC VALUE OF INTERNAL AUDIT	34
8.3.2	RESPONSIBILITIES OF INTERNAL AUDIT.....	34
8.3.3	STRATEGIC VALUE OF AUDITOR GENERAL	35
8.3.4	RESPONSIBILITIES OF EXTERNAL AUDIT	35
8.4	RISK MANAGEMENT OVERSIGHT	35
8.4.1	STRATEGIC VALUE OF RISK MANAGEMENT COMMITTEE	35
8.4.2	RESPONSIBILITIES OF THE RISK MANAGEMENT COMMITTEE	36
8.4.3	STRATEGIC VALUE OF THE AUDIT COMMITTEE	36
8.4.4	RESPONSIBILITIES OF THE AUDIT COMMITTEE	36
8.4.5	STRATEGIC VALUE OF THE ACCOUNTING OFFICER.....	36
8.4.6	RESPONSIBILITIES OF THE ACCOUNTING OFFICER.....	37
8.4.7	STRATEGIC VALUE OF EXECUTIVE AUTHORITY	37
8.4.8	RESPONSIBILITIES OF EXECUTIVE AUTHORITY	37
9.	RECOMMENDATIONS AND APPROVAL	38

ACRONYMS

AO – Accounting Officer

CAE – Chief Audit Executive (Head of Internal Audit Services)

COSO – The Committee of Sponsoring Organisations of the Treadway Commission

CRO – Chief Risk Officer (Head of Risk Management Unit)

ERM – Enterprise Risk Management

FMCMM – Financial Management Capability Maturity Model

HoD – Head of department

MEC – Member of Executive Council

PFMA – Public Finance Management Act

POE – portfolio of evidence

PT – Provincial Treasury

RMC – Risk Management Committee

SMS – Senior Management Services

TR – Treasury Regulations

DEFINITION OF TERMS AND CONCEPTS

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

Cost of risk – Costs associated with:

- Insurance premiums
- Incurred losses
- Loss control expenses including safety, security, property conservation, quality control programs, etc.
- Administrative costs (internal and external) including risk management component, internal claims (staff), fees paid to brokers, risk management consultants, outside claims and loss control services, including your time as risk manager and claims administrator

Enterprise risk management – is a process, effected by an entity's executive management (board of directors), management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives

Event – Occurrence of a particular set of circumstances

Impact or Severity or Consequence – Outcome of an **event**

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

Likelihood/Probability – Extent to which the **event** is likely to occur

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

Risk Communication – Exchange or sharing of information about risk between the decision-maker and other stakeholders

Risk Criteria – Terms of reference by which the significance of a risk is assessed

Risk Perception – Way in which a stakeholder views a risk based on a set of values or concerns

Risk Tracking – The monitoring of key risks over time to determine whether the level of risk is changing.

Source/Cause – Activity having a potential for a consequence

TERMS RELATED TO RISK TREATMENT AND CONTROL

Risk Acceptance – Decision to accept a risk

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

Risk Control – Actions implementing risk management decisions

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

Risk Reduction – Actions taken to lessen the probability of negative consequences 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

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

Mitigation – Minimising any negative consequence of a particular event

Residual Risk – The level of risk remaining after risk treatment

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

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 Assessment – Overall process of risk analysis and risk evaluation in order to identify potential opportunities or minimise loss.

Risk Evaluation – Process of comparing the estimated risk against given risk criteria to determine the significance of the risk

Risk Estimation – Process used to assign values to the probability and consequences of a risk

Risk Identification – Process to find, list and characterise elements of risk

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

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) – Head of Risk Management

Risk Champions – Officials drawn from programs to assist management in their risk management responsibilities.

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

LIST OF FIGURES AND TABLES

FIGURE NUMBER	NAME OF FIGURE
<i>Figure 1</i>	<i>Enterprise Risk Management Process</i>
<i>Figure 2</i>	<i>An Overview of Enterprise Risk Management Process & Escalation Matrix</i>
TABLE NUMBER	NAME OF TABLE
<i>Table 1</i>	<i>External Factors</i>
<i>Table 2</i>	<i>Internal Factors</i>
<i>Table 3</i>	<i>Impact/Consequences Parameters</i>
<i>Table 4</i>	<i>Likelihood Parameters</i>
<i>Table 5</i>	<i>Perceived Control Effectiveness</i>
<i>Table 6</i>	<i>Inherent Risk Rating Matrix</i>
<i>Table 7</i>	<i>Risk Rating Scale</i>
<i>Table 8</i>	<i>Residual Risk Exposure</i>
<i>Table 9</i>	<i>Overview of Risk Management Strategies</i>
<i>Table 10</i>	<i>Action Plans Implementation Ratings / Status</i>

1. INTRODUCTION

Risk management is implemented through the Risk Management Strategy and Implementation Plan, herein after referred to as the Strategy. The Strategy gives effect to the implementation of the department's Enterprise Risk Management Policy and its risk profile. The Strategy would be reviewed on an annual basis to ensure that it keeps up with developments in risk management.

2. OBJECTIVE

The Strategy was prepared to give effect to the implementation of the Enterprise Risk Management Policy and Enterprise Risk Management Committee Charter. The following objectives for the Risk Management Unit were developed:

- 2.1 Raising awareness of risk management and ensuring that guidelines are developed in compliance with applicable legislation and prescripts;
- 2.2 Risk identification, assessment and risk response at organisational, programme and functional levels of the DRDAR;
- 2.3 Identification and management of health and safety risks, injury prevention, reporting and management of incidents as well as compliance with the requirements of the Occupational Health & Safety Act

3. APPROACH

The development of the Enterprise Risk Management Strategy has taken into consideration:

- a. The Enterprise Risk Management Policy;
- b. The Risk Management Committee Charter

4. RISK MANAGEMENT MATURITY

The department must ensure that the following are achieved and maintained:

- a. Risk Management must be integrated into all operations, processes and planning of the department;
- b. The ERM Policy, Risk Management Strategy and Implementation Plan must be developed, approved, reviewed and implemented in line with their objectives;
- c. The Risk Management Committee must be fully operational and functional and operate in terms of its approved charter;
- d. Risk Management must be included in the performance agreements of all identified relevant personnel;
- e. Risk Management Unit must be adequately capacitated and resourced;
- f. ERM must be monitored effectively;
- g. ERM reports must be submitted regularly, reviewed and feedback given to programs for improvement; and

- h. Continuous training and awareness programmes must be conducted to employees of the department on ERM Policy, Strategy and Implementation Plan.

5. RISK CATEGORIES

As the risk environment is so varied and complex it is useful to group potential events into risk categories. By aggregating events horizontally across an institution and vertically within operational units, allows the development of an understanding of the interrelationship between events to gain enhanced information as a basis for risk assessment.

The main categories to group individual risk exposures are provided below:

RISK TYPE	RISK CATEGORY	DESCRIPTION
Internal	1. Human Resources	Risks that relate to human resources of an institution. These risks can have an effect on an institution's human capital with regard to: <ul style="list-style-type: none"> • Integrity and honesty; • Recruitment; • Skills and competence; • Employee wellness; • Employee relations; • Retention; and • Occupational health and safety.
	2. Knowledge and information management	Risks relating to an institution's management of knowledge and information. In identifying the risks consider the following aspects related to knowledge management: <ul style="list-style-type: none"> • Availability of information; • Stability of the information; • Integrity of information data; • Relevance of the information; • Retention; and • Safeguarding.
	3. Litigation	Risks that the institution might suffer losses due to litigation and lawsuits against it. Losses from litigation can possibly emanate from: <ul style="list-style-type: none"> • Claims by employees, the public, service providers and other third party • Failure by an institution to exercise certain rights that are to its advantage
	4. Loss \ theft of assets	Risks that an institution might suffer losses due to either theft or loss of an asset of the institution.
	5. Material resources (procurement risk)	Risks relating to an institution's material resources. Possible aspects to consider include: <ul style="list-style-type: none"> • Availability of material; • Costs and means of acquiring \ procuring resources; and • The wastage of material resources

RISK TYPE	RISK CATEGORY	DESCRIPTION
	6. Service delivery	Every institution exists to provide value for its stakeholders. The risk will arise if the appropriate quality of service is not delivered to the citizens.
	7. Information Technology	The risks relating specifically to the institution's IT objectives, infrastructure requirement, etc. Possible considerations could include the following when identifying applicable risks: <ul style="list-style-type: none"> • Security concerns; • Technology availability (uptime); • Applicability of IT infrastructure; • Integration / interface of the systems; • Effectiveness of technology; and • Obsolescence of technology.
	8. Third party performance	Risks related to an institution's dependence on the performance of a third party. Risk in this regard could be that there is the likelihood that a service provider might not perform according to the service level agreement entered into with an institution. Non-performance could include: <ul style="list-style-type: none"> • Outright failure to perform; • Not rendering the required service in time; • Not rendering the correct service; and • Inadequate / poor quality of performance.
	9. Health & Safety	Risks from occupational health and safety issues e.g. injury on duty; outbreak of disease within the institution.
	10. Disaster recovery / business continuity	Risks related to an institution's preparedness or absence thereto to disasters that could impact the normal functioning of the institution e.g. natural disasters, act of terrorism etc. This would lead to the disruption of processes and service delivery and could include the possible disruption of operations at the onset of a crisis to the resumption of critical activities. Factors to consider include: <ul style="list-style-type: none"> • Disaster management procedures; and • Contingency planning.
	11. Compliance \ Regulatory	Risks related to the compliance requirements that an institution has to meet. Aspects to consider in this regard are: <ul style="list-style-type: none"> • Failure to monitor or enforce compliance; • Monitoring and enforcement mechanisms; • Consequences of non-compliance; and • Fines and penalties paid.
	12. Fraud and corruption	These risks relate to illegal or improper acts by employees resulting in a loss of the institution's assets or resources.
	13. Financial	Risks encompassing the entire scope of general financial management. Potential factors to consider include: <ul style="list-style-type: none"> • Cash flow adequacy and management thereof;

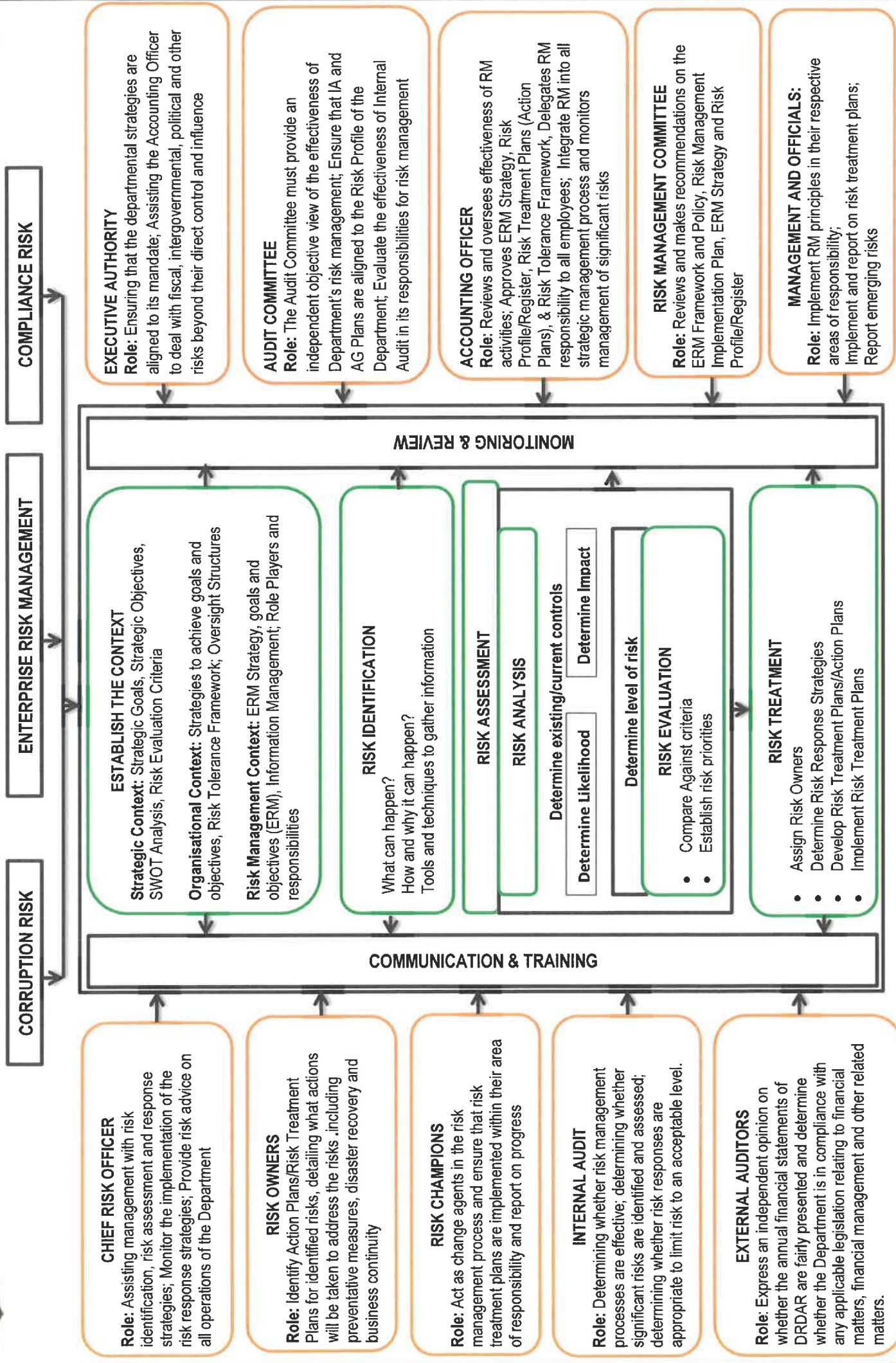
RISK TYPE	RISK CATEGORY	DESCRIPTION
		<ul style="list-style-type: none"> • Financial losses; • Wasteful expenditure; • Budget allocations; • Financial statement integrity; • Revenue collection; and • Increasing operational expenditure.
	14. Cultural	<p>Risks relating to an institution's overall culture and control environment. The various factors related to organisational culture include:</p> <ul style="list-style-type: none"> • Communication channels and the effectiveness; • Cultural integration; • Entrenchment of ethics and values; • Goal alignment; and • Management style.
	15. Intergovernmental and Interdepartmental Co-ordination Risks	Risks emanating from the relationship between the spheres of government in National, Provincial and Local levels as well as between provincial departments, and are having the effect of impeding the attaining of objectives
	16. Infrastructure Risks	Risks relating to infrastructure e.g. roads, buildings, dipping tanks, etc.
	17. Process/operational	Ineffective and inefficient processes. Inadequate controls in the operational processes.
	18. Project risks	Risks associated with not meeting project scope, costs, duration and deliverables
	19. Reputation	Factors that could result in the tarnishing of an institution's reputation, public perception and image.
External	20. Economic Environment	<p>Risks related to the institution's economic environment. Factors to consider include:</p> <ul style="list-style-type: none"> • Inflation; • Foreign exchange fluctuations; and • Interest rates.
	21. Political environment	<p>Risks emanating from political factors and decisions that have an impact on the institution's mandate and operations. Possible factors to consider include:</p> <ul style="list-style-type: none"> • Political unrest; • Political interference; • Local, Provincial and National elections; and • Changes in office bearers.
	22. Social environment	<p>Risks related to the institution's social environment. Possible factors to consider include:</p> <ul style="list-style-type: none"> • Unemployment; and • Migration of workers.
	23. Natural environment	<p>Risks relating to the institution's natural environment and its impact on normal operations. Consider factors such as:</p> <ul style="list-style-type: none"> • Depletion of natural resources;

RISK TYPE	RISK CATEGORY	DESCRIPTION
		<ul style="list-style-type: none"> • Environmental degradation; • Spillage; and • Pollution.
	24. Technological environment	Risks emanating from the effects of advancements and changes in technology.
	25. Legislative environment	Risks related to the institution's legislative environment e.g. changes in legislation, conflicting legislation.

6. ENTERPRISE RISK MANAGEMENT FRAMEWORK

In order for ERM to be effective, it relies on various interrelated and inter-dependent components as outlined in the following diagram:

Figure 1: DRDAR ENTERPRISE RISK MANAGEMENT FRAMEWORK



7. RISK MANAGEMENT PROCESS

Risk management is a systematic and a continuous process of identifying and analysing risks and, where appropriate, taking adequate steps to address these risks before they can impact negatively on service delivery capacity.

It is a management approach that increases prospects of success through getting-it-right-the-first-time and minimizing negative outcomes. It forms part of management's core responsibilities and is an integral part of DRDAR's internal processes. The process of risk management systematically follows the following steps:

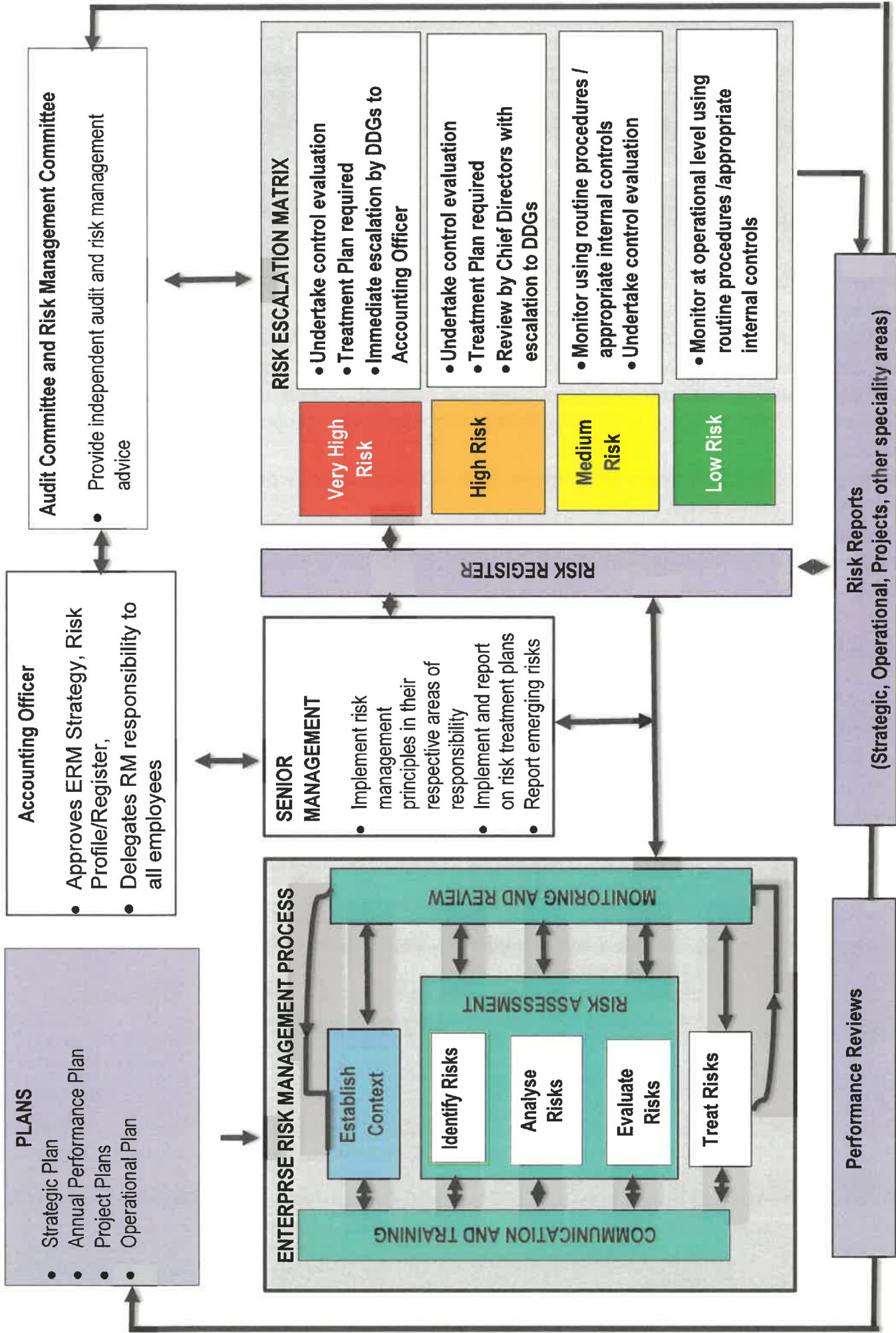


Figure 2: An Overview of Enterprise Risk Management Process and Risk Escalation Matrix

7.1 STEP 1: ESTABLISH THE CONTEXT

This process occurs within the strategic context and immediately follows the objective setting and business planning process. It is undertaken to define the basic parameters within which risks must be managed, and sets the scope for the risk management process. This step comprises of the following areas:

7.1.1 ESTABLISH STRATEGIC CONTEXT

The context includes financial, operational, competitive, political, reputational, social, cultural and legal aspects of the department's functions. It involves:

- i. Defining the relationship between the department and its environment;
- ii. Identifying institutional strengths, weaknesses, opportunities and threats;
- iii. Identifying internal and external stakeholders, and considering their objectives, take into account their perceptions, and establishing communication processes with these parties;
- iv. Determining crucial elements which might support or impair the department's ability to manage the risks it faces;
- v. Ensuring that there is a close relationship between the department's mission, strategic objectives and the management of all risks to which DRDAR is exposed.

Risks must be identified considering both internal and external factors as indicated below:

Table 1: External Factors

EXTERNAL FACTORS	Economic and Business	Related risks might include emerging or movements in the international, national, provincial markets and globalisations
	Natural environment	Risks might include such natural disasters as flood, fire or earthquake, and sustainable development.
	Political	Risks might include newly elected government officials and new legislation and regulations. The influence of international governments and other governing bodies
	Social	Risks might include changing demographics, shifting of family structures, work/life priorities, social trends and the level of citizen engagement
	Technological	Risks might include evolving electronic commerce, expanded availability of data and reductions in infrastructure costs.

Table 2: Internal Factors

INTERNAL FACTORS	Infrastructure	Risks might include unexpected repair costs, or equipment incapable of supporting production demand.
	Human resource	Risks might include increase in number of on-the-job accidents, increased human error or propensity for fraudulent behaviour.
	Process	Risks might include product quality deficiencies, unexpected downtime, or service delays.
	Technology	Risks might include inability to maintain adequate uptime, handle increased volumes, deliver requisite data integrity, or incorporate needed system modifications.
	Governance and accountability frameworks	Values and ethics, transparency, Policies, procedures and processes

7.1.2 ESTABLISH ORGANISATIONAL CONTEXT

Before a risk management activity is commenced, it is necessary to understand the institution and its capabilities, as well as its goals and objectives and the strategies that are in place to achieve them. Therefore:

- i. Risk management will take place in the context of wider goals, objectives and strategies of the department;
- ii. Inadequate or poor performance in delivering on the objectives of the department or specific activities, or projects is one set of risks which shall be managed;
- iii. The ERM Strategy defines the criteria by which it is decided whether a risk is acceptable or not, and form the basis for risk treatment.

7.1.3 ESTABLISH A RISK MANAGEMENT CONTEXT

The goals, objectives, scope and/or parameters of the activities to which the risk management process is being applied, shall be established. The process shall be undertaken with full consideration of the need to balance costs, benefits and opportunities. The resources required and the records to be kept shall also be specified. Setting the scope and boundaries of the risk management process will involve:

Defining the extent and comprehensiveness of the risk management activities to be carried out. Specific issues which will be considered include the following:

- i. The roles and responsibilities of various stakeholders of the department participating in managing risk;
- ii. Relationships between risk management; the strategic objectiveness or projects of the department;
- iii. Determination of interdependencies and relationships between the risk areas, i.e. how the risk areas impact on one another.

7.1.4 DEVELOP RISK EVALUATION CRITERIA

The Accounting Officer shall decide on criteria against which risk is to be evaluated. Decisions concerning risk acceptability and risk treatment shall be based on operational, technical, financial, legal, social, humanitarian or other criteria, depending on strategic objectives, legislation, regulations and the interests of stakeholders. Through the risk tolerance framework and the materiality & significance framework, risk evaluation criteria shall be further refined as particular risks are identified and risk analysis techniques chosen to ensure that the risk criteria corresponds with the type of risks and the way in which risk levels are expressed.

Table 3: Impact/Consequences parameters

		IMPACT / CONSEQUENCES				
		1 - Insignificant	2 - Minor	3 - Moderate	4 - Major	5 - Critical
Health and Safety	First Aid case	Minor injury, Medical case	Serious injury	Major or multiple injuries permanent injury or disability	Single or multiple fatalities	
Financial	< R500 000	R500 001 – R1 m	R1 m – R1.5 m	R1.5 – R2.5 m	>R2.5 m	
Schedule	Up to 3 days	3 days – 1 week	1 week – 1 month	1 – 2 months	> 2 months	
ICT Downtime	Up to 2 hours	2 – 3 hours	3 – 4 hours	5 – 8 hours	>1 day	
Reputation	Public concern restricted to local complaints.	Mostly repairable. Minor, adverse local media attention and complaints	Attention from media and/or heightened concern by local community. Criticism by NGOs.	Significant adverse national media/public/ NGO attention	Serious public or media outcry international coverage.	
Legal	Legal costs against budget 1%	Legal costs against budget 3%	Legal costs against budget 5%	Legal costs against budget 10%	Legal costs against budget <10%	
Operational / Business Impact	Impact can be absorbed through normal activity	An adverse event which can be absorbed with some management effort	A serious event which requires additional management effort	A critical event which requires extraordinary management effort	Disaster with potential to lead to collapse of project	

Table 4: Likelihood parameters

LIKELIHOOD/PROBABILITY RATINGS (LIKELIHOOD OF RISK EVENT OCCURRING)		
Likelihood	Rating	Description
Rare	1	Event may occur in exceptional circumstances, but there is little opportunity for it occurring.
Unlikely	2	Based on current information, the event is unlikely to occur although it has occurred within other organizations.
Possible	3	There is a strong possibility that the event can occur at some time within the business operating environment and/or the project lifecycle.
Likely	4	Based on the circumstances the event is very likely to occur. It has previously occurred and holds a high risk impact
Certain	5	As the circumstances which cause the risk to eventuate are almost certain to occur, the opportunity or the event to occur is very high.

7.2 STEP 2: RISK IDENTIFICATION

The process of risk identification shall involve utilisation of various techniques and models to ensure that no critical risks are missed out. The following approaches shall be utilised:

7.2.1 OBJECTIVE BASED RISK ASSESSMENT MODEL

The best people to identify risks using this method are those who are expected to implement the objectives because they are aware of the various activities, opportunities and challenges in implementing the objectives. The objective-based risk assessment model follows the following process:

a. Defining the objectives

The overall perspective of objectives is defined in the Strategic Plan of the department. Management therefore shall define objectives based on the strategic priorities identified in the strategic plan depending on where they fit into the bigger picture.

b. Articulating the objectives

In order to ensure successful operationalization of the strategic plan programmes need to establish:

- i. What specifically needs to be achieved?
- ii. What the intended outcome is?
- iii. What the foundational assumptions are to achieve it?

This process shall result in the annual performance plan and operational plan of the programmes.

c. Measurable outcomes

Programmes shall establish how success will be measured by assigning performance indicators to each specific objective.

d. Achievement status

Looking backwards on the operations of the programmes, management shall establish how programmes have performed over time in order to determine their status of achieving each objective and to prioritise each objective relative to each other.

e. Assessing the risks

During this step management identifies the main uncertainties that can have a major impact on the objectives. External uncertainties are usually beyond management control, however, management shall develop business continuity plans to alleviate the impact of these uncertainties. What can prevent achievement of objectives and what can aid achievement of objectives shall also be identified by conducting SWOT analysis for the department. For this step to be undertaken successfully, the following data sources shall be utilised:

i. Process Mapping

Process mapping shall be used to identify interdependent, critical and vulnerable functions and activities in all high risk areas.

ii. Business Impact Analysis (BIA) reports

Business Impact Analysis reports shall be developed and utilised as reference documents in the risk assessment process.

iii. Brainstorming

Brainstorming is a technique of solving specific problems, amassing information, stimulating creative thinking, developing new ideas, etc. by unrestrained and spontaneous participation in discussions. This shall be done through facilitated workshops to provide meaningful information in the risk assessment process.

iv. Document Review

Review of the institution's internal policies; operational reports and procedure manuals shall also provide useful information on the risks the department may be faced with as well as an understanding of what risk treatment strategies would work best for the department.

v. Internally Generated Data / Historical Experiences

Analysing information from Annual Reports, financial statements, loss control reports, incident reports, corruption database, litigation register, etc. shall be utilised to predict future events. This is the most effective approach as it provides better unbiased results and a basis for risk rating.

vi. Market Research & Relevant Published Material

Understanding what is happening in global markets and how it affects the sector or operations of the department shall be critical to ensure that risk identification is conducted appropriately. Although it is outside the control of the department to prevent systemic risks, management shall develop business continuity plans to ensure recovery in the event of a systemic risk materialising.

vii. Specialist Expert Judgements

Specialist areas such as health & safety; scientific research & IT will require expert judgement to identify risks in these areas adequately. Internal and External Audit reports shall provide a specialist and independent insight into the department.

7.2.2 SCENARIO PLANNING

Scenario planning shall be used as an additional methodology to identify project related risks in the following process.

a) Identification of external forces

From several external forces related-changes which might impact the project are imagined, e.g. change in regulations, demographic changes, topical issues and headlines.

b) Predicting the future

For each of the external forces chosen above, management consider three different future scenarios which might arise within the project or the institution as a result of each change. These shall include best-case, worst-case and reasonable-case scenarios. The worst-case scenario shall be reviewed against the department's risk tolerance to determine what changes need to be made to survive this period or turn things around.

c) Determination of response action

What the project manager might do or potential strategies to respond to each of the scenarios are determined.

d) Identification of risk treatment considerations

Common considerations and issues that must be addressed to respond to possible external changes are detected.

e) Selection of robust response strategies

The most likely external changes to affect the project are identified and the most reasonable strategies project managers can undertake to respond to the changes are selected.

7.2.3 ENVIRONMENTAL SCANNING

Environmental scanning is a process of identifying emerging issues, situations, and potential pitfalls that may affect an organisation's future. It increases the organisation's awareness of the key risks it faces, and the characteristics and attributes of these risks. This method enables decision makers both to understand the external environment and interconnections of its various sectors and to translate this understanding into the institution's planning and decision making processes; therefore it shall be used to:

- i. Detect scientific, technical, economic, and social trends and events important to the institution;
- ii. Define the potential threats, opportunities, or changes for the institution implied by those trends and events;
- iii. Promote a future orientation in the thinking of management and staff; and

- iv. Alert management and staff to trends that are converging, diverging, speeding up, slowing down or interacting.

Key questions that shall be considered in undertaking this analysis include:

- a) This **type** of risk, i.e. IT/Systems, Financial, Health & Safety, Corruption, etc.
- b) The **source** of the risk, i.e. external (political, economic, natural disasters) or internal (inadequate resources, security, knowledge management, etc.);
- c) **What** is at risk, i.e. areas of impact in the event that risk materialises and the type of exposure (people, reputation, service delivery, finances, materials, etc.)
- d) The **existing controls and their effectiveness**, i.e. the degree to which the department can influence, affect or manage the risk.

Understanding the organisational context and conducting an environmental scan shall assist the department in identifying key risk areas and differentiating between the types of risks, i.e. specific event risks and risks that cut across the entire organisation (transversal risks). The scan shall also provide the department with meaningful information to set a strategic direction for risk management which can be amended or adjusted, as more information comes to light, or as the capacity to manage risks increases.

7.2.4 RISK PROFILES

Risk profiles shall be developed and reviewed on an annual basis. Three levels of risk profiles need to be developed and maintained by the department. These are:

- Strategic;
- Operational; and
- Project



Figure 3: Risk Profiles

The development and maintenance of the profiles must be a continuous process but management should formally assess and agree on the profiles annually. This is usually achieved through

facilitated workshops where management collectively agrees on the risk identification, assessment and actions.

7.3 STEP 3: RISK ASSESSMENT

The process of risk assessment shall involve risk analysis and risk evaluation as follows:

7.3.1 RISK ANALYSIS REVIEW

The objective of risk analysis is to separate minor acceptable risks from the major risks, and to provide data to assist in the evaluation and treatment of risks. Risk treatment considers the sources of the risk, their consequences (impact) and the likelihood that those consequences may occur. During this stage risk is combining estimates of impact and likelihood in the context of existing control measures.

a) Determine existing controls

Identify existing management technical systems and procedures to control risk and assess their strengths and weaknesses.

b) Impact and likelihood

Each risk is rated in terms of impact and likelihood to determine the inherent risk rating. This rating is done without considering the controls that may be in place. The effectiveness of the existing risk responses (current controls) is assessed for these risks. This is done by rating the perceived control effectiveness as per the table below, against the inherent risk to determine the residual risk (remainder of risk after applying controls). A decision is then needed to determine if the risk falls within the desired levels of risk appetite.

Table 5: Perceived Control Effectiveness

Perceived Control Effectiveness Ratings:			
Control Effectives	Rating 1-5	Description	Calculation of the control effectiveness Rating
Very good	1	Nothing more to be done except review and monitor the existing controls. Controls are well designed for the risk, and address the root causes. Management believes they are effective and reliable at all times.	10%
Good	2	Most controls are designed correctly and are in place and effective. Some more work to be done to improve operating effectiveness or management has doubts about operational effectiveness and reliability.	20%

Perceived Control Effectiveness Ratings:

Control Effectives	Rating 1-5	Description	Calculation of the control effectiveness Rating
Satisfactory	3	While the design of controls may be largely correct in that they treat most of the root causes of the risk, they are not currently very effective. / Some of the controls do not seem correctly designed in that they do not treat root causes. Those that are correctly designed are operating effectively.	65%
Weak	4	Significant control gaps. Either controls do not treat root causes or they do not operate at all effectively.	80%
No Controls	5	No controls identified	100%

“Overall Control Rating” relates to the perceived design adequacy and operating effectiveness of the combined controls deployed by determining whether they are sufficient enough to mitigate the impact of the risk in the event of it occurring.

To avoid subjective biases sources of information shall include the following:

- i. Past records;
- ii. Loss events and incident register;
- iii. Corruption database;
- iv. Relevant experience;
- v. Industry practice and experience;
- vi. Relevant published literature;
- vii. Specialist and expert judgements.

Where no past data is available, subjective estimates shall be made to reflect the degree of belief that a particular event or outcome will occur. To avoid subjective biases the best available information sources and techniques shall be used when analysing impact and likelihood.

c) Risk analysis techniques

Techniques for risk analysis shall include:

- i. Structured interviews with experts in the area of interest;
- ii. Individual evaluation using questionnaires.

d) Types of risk analysis

Risk analysis shall be undertaken to various degrees of refinement depending upon the risk information and data available. Analysis of risks shall be qualitative or quantitative or a combination of these, depending on the circumstances. Initially qualitative analysis shall be used to obtain a general indication of the level of risk. Where it is necessary to undertake more specific quantitative analysis based on the nature of significant risks identified, quantitative analysis shall be performed.

i. Qualitative analysis

Qualitative risk analysis uses word form or descriptive scales to describe the magnitude of potential impact and the likelihood that those risks will occur. The qualitative analysis is then depicted through a matrix in which risks are assigned to priority classes by combining their likelihood and consequence. Risk impact on the ability of the department to deliver on its mandate shall be highlighted in the following categories:

- **Financial:** The impact of risks to the department's financial stability and ability to maintain funding critical activities to deliver on its strategic objectives;
- **Materials:** The impact of the risk on material resources and infrastructure such as equipment, machinery, vehicles, tec. that the department uses in the activities that are critical to its mission;
- **People:** The impact of the risk on the department's workplace and other stakeholders;
- **Reputation:** The impact of the risk on the public's perception of the department and its stakeholders; and
- **Service Delivery:** The impact of the risk on service delivery, e.g. project completion.

ii. Quantitative analysis

Quantitative analysis uses numerical values (rather than the descriptive scales used in qualitative analysis) for both impact and likelihood using data from a variety of sources. The quality of the analysis will depend on the accuracy and completeness of the numerical values used. Risk impact shall be estimated by modelling outcomes of an event or set of events or by extrapolation past data and expressed in the same categories as qualitative analysis.

e) Risk Matrix

A risk rating matrix shall be utilised to determine the extent of the risk exposure the department is faced with in order to allocate the appropriate response to that specific risk. Management shall decide on actions that need to be taken to address the risk based on the following guidelines endorsed by the Accounting Officer:

APPLYING THE PARAMETERS TO THE RISK MATRIX TO INDICATE WHAT AREAS OF THE RISK MATRIX WOULD BE REGARDED AS LOW, MEDIUM, HIGH OR VERY HIGH RISKS:

Table 5: Inherent Risk Rating Matrix: Risk rating index = impact x likelihood

		Risk Impact					
		5	10	15	20	25	
Severe							Very High Risk
Major							Very High Risk
Moderate							High Risk
Minor							High Risk
Minimal							Medium Risk
Risk Rating Matrix		Rare	Unlikely	Possible	Likely	Certain	

Risk Likelihood

Risk Likelihood

Table 7: Risk Rating Scale

Risk Rating Scale (Calculated Ratings of Likelihood and Impact)	
Rating 1-3	Low Risk
Rating 4-6	Medium Risk
Rating 8-12	High Risk
Rating 15-25	Very High Risk
	A risk event with a very low chance of occurrence, but if it does occur it can be managed under normal conditions
	Likely to occur- Risk which can be managed but requires additional resources and management effort in order to ensure that objectives/project deliverables are achieved
	Highly likely to occur- Potentially significant risk exposure that can be endured, but it will have prolonged negative impact and extensive consequences on objectives/project
	Almost certain to occur- The risk is potentially disastrous, could fundamentally hinder the achievement of the objectives and ultimately lead to the collapse of the business/project

7.3.2 RISK EVALUATION

Risk evaluation involves comparing the level of risk found during the analysis process with previously established risk criteria. Risk analysis and the criteria against which risks are compared in risk evaluation shall be considered on the same basis. The output of a risk evaluation is a prioritised list of risks for further action. The objectives of the department and extent of opportunity which could result from taking the risk shall be considered.

Table 8: Residual Risk Exposure

Risk exposure	Risk acceptability	Proposed actions	Factor
Very High Risk	Unacceptable	Take action to reduce risk with highest priority, Inform Head of Department	15 - 25
High Risk	Unacceptable	Take action to reduce risk with highest priority, inform DDG/s	8.0 – 14.9
Medium Risk	Partially Acceptable	Take action to reduce risk, inform Chief Directors	4.0 – 7.9
Low Risk	Acceptable	No risk reduction - control, monitor	1 – 3.9

7.4 STEP 4: RISK TREATMENT

Risk treatment involves identifying a range of options for risk response, assessing those options, preparing risk treatment plans and implementing them. Risk treatment involves the following processes:

7.4.1 ASSIGNMENT OF RISK OWNERSHIP

Risk owners shall be appointed by the Accounting Officer and their main responsibility shall be the development of risk treatment plans for the adopted risks. Risk Owners shall preferably be nominated from senior management and must have sufficient technical knowledge about the risk and/or risk area for which a response is required; they shall also have authority to delegate risk treatment actions to officials within and outside their management scope, however, will remain accountable for the management of allocated risks.

Determination of risk response strategies. Risk Response comprises of different strategies, such as:

a. Avoidance / Terminate

Taking action to eliminate the activities that give risk to the risk such as ceasing the activity or changing the objective.

b. Reduction / Treat

Taking action to reduce either the likelihood or impact of a risk or both such as; influencing regulations and public perception; implementing business continuity plans; or reorganising and restructuring.

c. Sharing / Transfer

Taking action (within the limitations of Treasury Regulation 12.1.1) to transfer the loss or liability to third parties through:

- i. Outsourcing; and
- ii. Partnerships

d. Acceptance / Tolerate

Risk acceptance refers to taking no action to affect likelihood or impact and is usually considered for low risks.

Management shall identify risk response strategies and consider their effect on risk likelihood and risk impact in relation to the institution’s risk tolerance and cost benefit analysis, and then design and implement risk treatment plans.

Table 9: Overview of Risk Management Strategies

Risk Index	Risk Management Strategies	Accountability
15 - 25	Avoid, reduce, share, or transfer the risk	DDGs/ Inform HOD
8.0 – 14.9	Reduce, share, or transfer the risk	Chief Directors/ Inform DDGs
4.0 – 7.9	Accept Partially and/or reduce risk. Monitor and address its impact and/or likelihood	Directors/ Inform Chief Directors
1 – 3.9	Accept the risk. Monitor and address its impact and/or likelihood	All/ Inform Management

7.4.2 DETERMINING THE RISK ACCEPTANCE CRITERIA BY IDENTIFYING WHAT RISKS WILL NOT BE TOLERATED

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.

Determining the risk acceptance criteria by setting risk acceptance levels. Defining a risk as acceptable does not imply that the risk is insignificant. The assessment should take into account the degree of control over each risk; the cost impact, benefits and opportunities presented by the risk and the importance of the policy, project, function or activity.

Reasons for classifying a risk to be acceptable could include:

- The likelihood and impact of the risk could be so low that specific treatment is inappropriate
- The risk being such that no treatment is available
- The cost of the treatment being so excessive compared to the benefit that acceptance is the only option.

7.4.3 DEVELOPMENT OF RISK TREATMENT PLANS

The purpose of the Risk Treatment Plans is to give DRDAR management and stakeholders, peace of mind that significant risks are being effectively managed and will help bring greater focus to the department's risk and planning arrangement. Key Risk Indicators (KRIs) for each risk shall be identified as part of the Risk Treatment Plans and submission dates for performance data shall be shown on these plans for reference.

7.4.4 IMPLEMENTING RISK TREATMENT PLANS

Responsibility for treatment of risk shall be borne by risk owners who are selected because they are best able to control the risk. To ensure successful implementation of risk treatment plans the Accounting Officer has delegated management to develop an effective management system which specifies the methods chosen, assigns responsibilities and individual accountabilities for actions, and monitors them against specific criteria.

Where after treatment there is a residual risk, a decision shall be taken based on the risk response framework as to whether to retain this risk or enhance the risk treatment process.

Table 10: Action Plans Implementation Ratings / Status

CORRECTIVE ACTION IMPLEMENTATION RATINGS	
PROGRESS RATING OF ACTION PLANS	ACTION PLAN PROGRESS EXPLANATIONS
Fully Implemented	The action has been fully executed and implemented.
Partially Implemented	The action is progressing as planned and is within target date.
Not Implemented	The action owner has not executed the action.

7.5 STEP 5: MONITORING AND REVIEW

Monitoring of risks shall encompass review of the effectiveness of risk treatment plans, strategies and the management system set up to control implementation. The objective of monitoring and review is to ensure that changing circumstances are incorporated in risk priorities and to ensure that the risk management plan remains relevant.

Factors which may affect the likelihood and consequences of an outcome may change, as may the factors which affect suitability or cost of the various treatment options, therefore regularity repeating the risk management process shall be necessary. Review is an integral part of the risk management treatment plan.

7.5.1 MONITORING

Monitoring of the presence and functioning of various elements required to ensure effectiveness of ERM shall be done in two ways, namely; ongoing monitoring of activities and separate evaluations. The monitoring process shall provide assurance that there are appropriate controls and that, policies and procedures are understood and followed.

a. Ongoing Monitoring Activities

Ongoing monitoring activities shall serve to monitor the effectiveness of risk management in the course of running the department's business. These shall include regular management and supervisory activities, variance analysis, performance evaluations, reconciliations and other routine actions.

b. Separate Evaluations

Separate evaluations shall be conducted periodically for significant risks by the Chief Risk Officer and the Internal Auditors focusing on the effectiveness and adequacy of controls as well as the overall effectiveness of risk management activities. Where deficiencies are identified, the relevant line managers shall on a continuous basis monitor the implementation of recommendations in order to evaluate their effectiveness. Where such risk management recommendations fail, they shall immediately report such failure to the CRO.

The CRO shall assist relevant heads of components or line managers in designing and implementing remedial measures to minimise the risk exposure whenever there is a need. The monitoring and review process shall also determine whether:

- i. Measures adopted resulted in what was intended;
- ii. Procedures adopted and information gathered for undertaking the assessment were appropriate;
- iii. Improved knowledge would have to reach better decisions and identify what lessons could be learnt for future assessments and management of risks.

7.5.2 REVIEW

Effective risk management requires a reporting and review structure to ensure that risks are effectively identified and assessed and that appropriate controls and responses are in place. Regular audits of policy and standards compliance shall be carried out and standards performance reviewed to identify opportunities for improvement. Bearing in mind that the department is an institution operating in dynamic environment; changes in the department and the environment shall be identified and appropriate modifications made to risk management systems.

7.6 STEP 6: COMMUNICATION AND TRAINING

It is important for risk reporting to demonstrate how well the department is management its key risks, this requires that risk reporting arrangements for all stakeholders must defined and communicated. A clearly defined structure shall facilitate effective communication among stakeholders in the risk management process.

A common risk language, consistent form of reporting and collaboration among stakeholders (Committees, Management, Chief Risk Officer, Internal Audit, etc.) is critical to ensure that risk reports are effectively utilised to drive institutional performance. While risk reporting is meant to aid managers to make risk based decisions, it is equally important for such information and decisions to be communicated to operational staff and/or relevant officials across the department.

Perceptions of risk can vary due to difference in assumptions and concepts and the needs, issues and concerns of stakeholders as they relate to the risk or the issues under discussion. Stakeholders are likely to make judgments of the acceptability of a risk based on their perception of the risk. Since stakeholders have a significant on the decisions made, their perceptions of risk, as well as their perceptions of benefits, shall be identified and documented and the underlying reasons for them understood and addressed.

Various sources of internal and external information shall be used to source data for reporting and this information could be in quantitative and/or qualitative form. The challenge to process and refine large volumes of data into relevant and actionable information; and to keep historic records of analysis, trends and decisions shall be overcome by information system to source, capture, process, analyse and report relevant information.

7.6.1 COMMUNICATION

a. Implementing a risk management information system

The use of a risk management information system will enable management to obtain “real time” information decision making. This will also enhance monitoring activities. Technology may provide the necessary audit trail that could be used by risk owners and assurance providers to determine whether controls are working effectively, including whether target dates for action plans are being fully complied with.

Although technology may provide value to risk reporting, the Chief Risk Officer shall ensure that processes around risk reporting are properly designed before implementation of technology is considered.

Customised reports shall be used as an early warning system. A risk dashboard shall be used to expedite the flow of critical information to enhance decision making. Supplementary information shall be included in more detailed reports such as progress with risk management implementation, incident reports, and emerging risk reports.

b. Incident reporting system

Incident reporting provides means of risk monitoring and reviewing the effectiveness of controls and the principle of real time incident reporting for key processes is growing in prominence globally. All Risk Owners must report incidents as DRDAR must maintain an Incident Register. Such reporting systems shall be integrated into the broader risk management reporting systems in order to avoid duplication of effort and enhance information sharing activities.

c. Emerging risks

Emerging risks are risks that were previously unrecognised but may be an imminent threat. Such risks may emanate through changes in the regulatory environment, external events, internal changes or social trends.

The risk management agenda of DRDAR shall incorporate process of identifying emerging trends, which could pose risks to the department. The frequency with emerging risks are interrogated will be influenced by the rate of change and dynamism the department is confronted with.

7.6.2 REPORTING

Effective internal and external communication is important to ensure that those responsible for implementing risk management, and those with a vested interest understand the basis on which decisions are made and why particular actions are required. Reporting on risk shall focus on both internal and external stakeholders.

7.6.2.1 INTERNAL REPORTING

Different stakeholders within the department require different types of risk information in different formats, therefore risk reports, although they will be based on a common risk language, shall be customised to cater for the needs of the different stakeholders. The following risk reporting responsibilities shall be carried out:

- a. The Chief Risk Officer (CRO) shall determine risk information needs of various stakeholders and ensure that risk management processes respond to such needs.
- b. After each risk assessment the CRO shall prepare and submit a draft risk register to the relevant Branch Heads, Programme Managers and Risk Owners identified during the risk assessment for comments, inputs and commitment on action plans.
- c. Once agreement has been reached on the contents of the risk register between the CRO and management, a detailed risk assessment report shall be prepared and submitted to the relevant managers for sign-off.
- d. The content and format of reports shall be determined by information requirements of different stakeholders as follows:

i. Accounting Officer

The Accounting Officer is accountable for risk management in the department and therefore should:

- a) Know about the significant risks facing the department;
- b) Be assured of appropriate levels of awareness throughout the department;
- c) Be assured that the risk management process is working effectively;
- d) Ensure that a risk management policy is developed covering risk management philosophy and responsibilities.

ii. Components and Programmes

DDGs, Programme Managers and Chief Directors are the risk managers and are expected to manage risks within their area of responsibility and make risk based decisions therefore they must:

- a) Be aware of the risks which fall into their areas of responsibility, the possible impacts these may have on other areas and the consequences other areas may have on them.
- b) Have performance indicators which allow them to monitor the key business activities, progress towards objectives and identify developments which require intervention have systems which communicate variances in budgets and forecasts at appropriate frequency to allow action to be taken;
- c) Report systematically and promptly to the CRO and Programme Managers any perceived new risks or failures of existing control measures.

iii. Other Employees

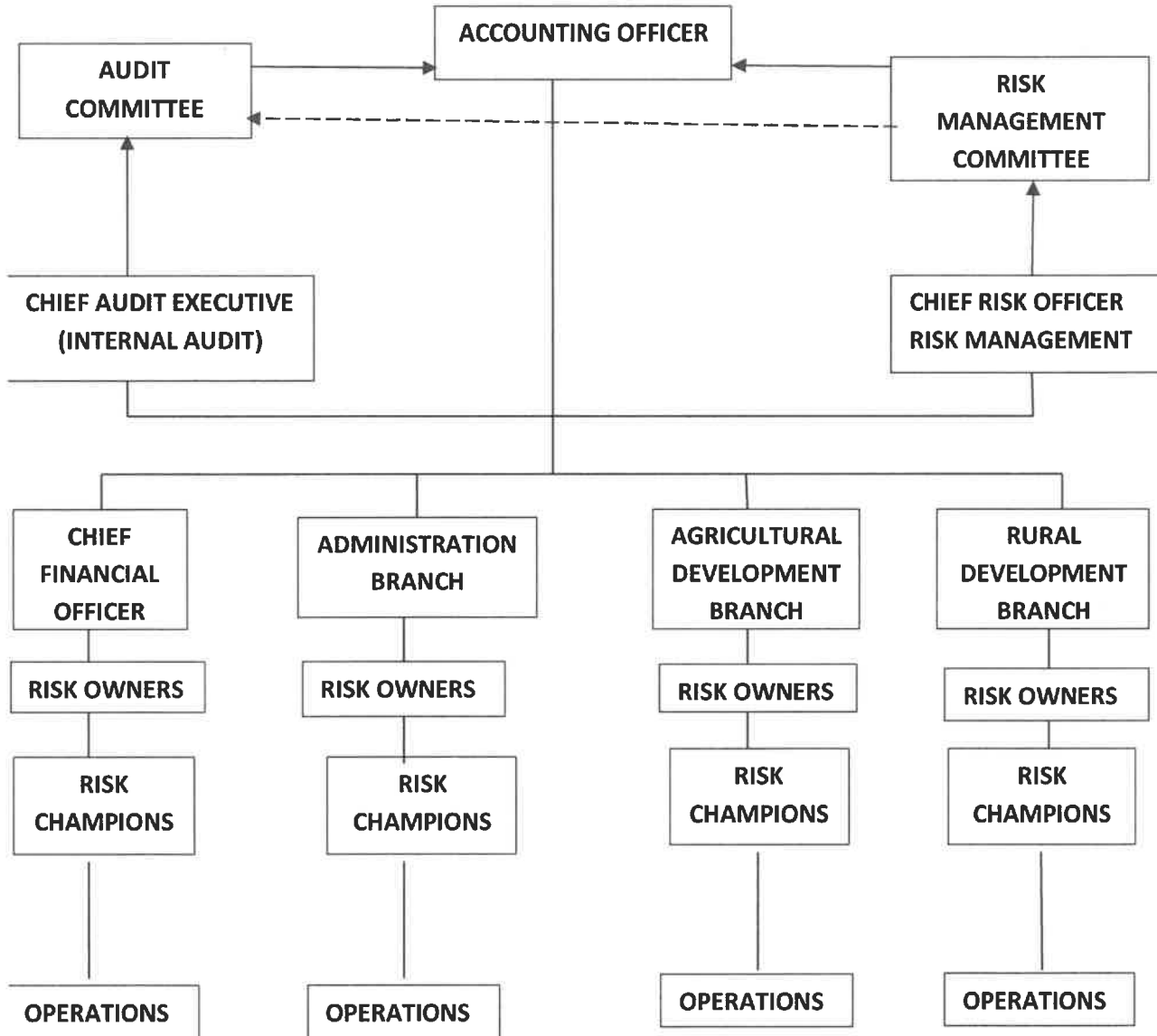
It is important that other employees are made aware of their risk management responsibilities because they are at the forefront of operations and as such can trigger risk through their actions or omissions, therefore they should:

- a) Understand their accountability for individual risks;

- b) Understand how they can enable continuous improvement of risk management response;
- c) Understand that risk management and risk awareness are a key part of the department's culture;
- d) Report systematically and promptly to senior management any perceived new risks or failure of existing control measures.

The following risk reporting structure shall be utilised to risk information within the department:

REPORTING TEMPLATE



Risk Champions are drawn from existing resources, from within the DDG Branches and operations

Risk Owners: Strategic Risks – DDGs, CFO and COO
Operational Risks – Chief Directors

Risk Champions: Strategic Risks – Chief Directors
Operational Risks – Directors, Deputy Directors and Assistant Directors

7.6.2.2 EXTERNAL REPORTING

Every organisation needs to report to its stakeholders on regular basis setting out its risk management policies and the effectiveness in achieving its objectives. Increasingly stakeholders look to organisations to provide evidence of effective management of the organisation's non-financial performance.

Good corporate governance principles require institutions to adopt a methodical approach to risk management which:

- a. Ensures that the Accounting Officer discharges his duties to direct strategy, builds value and monitors performance of the department;
- b. Ensures that management controls are in place and are performing adequately.

Through the annual report, formal reporting of risk management is made available to DRDAR stakeholders. The formal process addresses:

- a. The control methods – particularly management responsibilities for risk management;
- b. The processes used to identify risks and how they are addressed by the risk management systems;
- c. The primary control systems in place to manage significant risks;
- d. The monitoring and review systems in place.

Any significant deficiencies uncovered by the risk management system, or within the system itself, shall be reported together with the steps taken to deal with them.

7.6.3 TRAINING

The ERM Unit is mandated to champion and promote risk management across the department and ensure that:

- a. All officials and managers are aware of what risk management is and what benefits will their responsibility for risk management is;
- b. All officials and managers are aware of DRDAR's approach to risk management and what their responsibility for risk management is;
- c. All officials and managers are aware of how risk management is implemented and how to participate in the implementation.

The Risk Management Unit shall make use of the following mechanisms to communicate the risk management message:

- a. Training and workshops;
- b. Intranet;
- c. Induction of new employees;
- d. Internal publications

8 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. Risk Management roles and responsibilities have been divided into four categories due to the unique responsibilities of the role-players in each category. The categories are as follows:

8.1 RISK MANAGEMENT IMPLEMENTERS

All management and other officials within DRDAR are risk management implementers. Their fundamental roles and responsibilities are as follows:

8.1.1 MANAGEMENT

8.1.1.1 STRATEGIC VALUE OF MANAGEMENT

Management is accountable for designing, implementing and monitoring a system of risk management, and integrating it into the day-to-day activities of the department. As such management must ensure that it is satisfied with the management of risk and prevent risk management from becoming a series of activities that are detached from the realities of the department's operations. Risk management, when integrated into the decision making process becomes a valuable strategic management tool for underpinning the efficacy of service delivery and value for money. Management must ensure that risk management is a standing agenda item in management meetings.

8.1.1.2 RESPONSIBILITIES OF MANAGEMENT

- 8.1.1.2.1 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.
- 8.1.1.2.2 Empowering officials to perform effectively in their risk management responsibilities through proper communication of responsibilities, comprehensive orientation and ongoing opportunities for skills development;
- 8.1.1.2.3 Aligning the functional risk management methodologies and processes and departmental processes;
- 8.1.1.2.4 Devoting personal attention to overseeing the management of key risks within their area of responsibility;
- 8.1.1.2.5 Maintaining a cooperative relationship with the Chief Risk Officer, Risk Management Unit, Risk Owners and Risk Champions;
- 8.1.1.2.6 With the help of the Risk Management Unit – identify risks within their line function;
- 8.1.1.2.7 Designing and implementing controls to mitigate identified risks;

- 8.1.1.2.8 Analyse controls for adequacy and effectiveness and implement corrective and improvement measures;
- 8.1.1.2.9 Maintaining the proper functioning of the internal control processes within their area of responsibility;
- 8.1.1.2.10 Monitoring risk management within their area of responsibility;
- 8.1.1.2.11 Implementing the directives of the Accounting Officer concerning risk management;
- 8.1.1.2.12 Providing risk management reports and presentations to the Risk Management Committee and Audit Committee as requested; and
- 8.1.1.2.13 Holding employees accountable for their specific risk management responsibilities.

8.1.2 OTHER EMPLOYEES

8.1.2.1 STRATEGIC VALUE OF OTHER OFFICIALS

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.

8.1.2.2 RESPONSIBILITIES FOR OTHER OFFICIALS

- 8.1.2.2.1 Applying risk management processes in their respective functions;
- 8.1.2.2.2 Implementing the delegated action plans to address identified risks;
- 8.1.2.2.3 Inform their supervisors and/or Risk Management Unit of new risks and significant changes in known risks;
- 8.1.2.2.4 Cooperate with other role players in the risk management process and provide information as required;
- 8.1.2.2.5 Adhering to the code of conduct and code of ethics of the public service;
- 8.1.2.2.6 Maintaining the functioning of internal control processes, information and communication as well as the monitoring systems within their area of responsibility
- 8.1.2.2.7 Participating in risk identification and risk assessment processes within their business unit;
- 8.1.2.2.8 Reporting inefficient, unnecessary and unworkable controls; and
- 8.1.2.2.9 Reporting suspicion of fraud and corruption to the Anti-corruption unit through the whistleblowing processes.

8.2 RISK MANAGEMENT SUPPORT

8.2.1 STRATEGIC VALUE OF RISK CHAMPIONS

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. The Risk

Champion also adds value to the risk management process by providing support to the CRO in terms of information requirements and reports.

8.2.2 RESPONSIBILITIES OF RISK CHAMPIONS

- 8.2.2.1 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;
- 8.2.2.2 The Risk Champion must not assume the role of Risk Owner but should assist the Risk Owner to resolve problems.

8.2.3 RISK OWNERS

- 8.2.3.1 Risk Owners are those officials responsible for controlling (fully or partly) one of the significant risks.
- 8.2.3.2 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.
- 8.2.3.3 Reports and portfolio of evidence for all risks within their responsibility would collated regularly (quarterly) and submitted to the CRO for review and comment.
- 8.2.3.4 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.

8.2.4 STRATEGIC VALUE OF CHIEF RISK OFFICER

The primary responsibility of the Chief Risk Officer is to assist the department to embed risk management and leverage its benefits to enhance performance.

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. 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.

8.2.5 RESPONSIBILITIES OF THE CHIEF RISK OFFICER

- 8.2.5.1 Working with senior management to develop the department's vision for risk management;
- 8.2.5.2 Developing, in consultation with management, the department's risk management framework incorporating inter alia:

- 8.2.5.2.1.1 Risk Management Policy;
- 8.2.5.2.1.2 Risk Management Strategy;
- 8.2.5.2.1.3 Risk Management Implementation Plan;
- 8.2.5.2.1.4 Risk identification and assessment methodology;
- 8.2.5.2.1.5 Risk appetite and tolerance
- 8.2.5.3 Communicating the department's risk management framework and Strategy to all stakeholders in the department and monitoring its implementation;
- 8.2.5.4 Facilitating orientation and training for the Risk Management Committee;
- 8.2.5.5 Training all stakeholders in their risk management functions;
- 8.2.5.6 Continuously driving risk management to higher levels of maturity;
- 8.2.5.7 Assisting management with risk identification, risk assessment and response strategies;
- 8.2.5.8 Monitor the implementation of the risk response strategies;
- 8.2.5.9 Collating, aggregating, interpreting and analysing the results of risk assessments to extract risk intelligence;
- 8.2.5.10 Reporting risk intelligence to the Accounting Officer, management and the Risk Management Committee; and
- 8.2.5.11 Participating with Internal Audit, Management, and Auditor General in developing the combined assurance plan for the department.
- 8.2.5.12 Provide risk advice on all operations of the Department.

8.3 RISK MANAGEMENT ASSURANCE PROVIDERS

8.3.1 STRATEGIC VALUE OF INTERNAL AUDIT

Internal Audit is responsible through the Audit Committee for providing independent assurance on the effectiveness of the system of risk management. Hence, Internal Audit shall evaluate the effectiveness of the entire system of risk management and provide recommendations for improvement where necessary.

Internal Audit shall pursue a risk based approach to audit planning as opposed to a compliance approach, in order to assess whether the processes intended to serve as controls are appropriate risk controls.

8.3.2 RESPONSIBILITIES OF 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:

- 8.3.2.1 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:
 - 8.3.2.1.1 Institutional objectives support and align with the Institution's mission;
 - 8.3.2.1.2 Significant risks are identified and assessed;
 - 8.3.2.1.3 Risk responses are appropriate to limit risk to an acceptable level; and

8.3.2.1.4 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.

8.3.3 STRATEGIC VALUE OF AUDITOR GENERAL

The Auditor General is the supreme audit institution (SAI) of South Africa. It is an independent institution with legal capacity and is subject only to the constitution and the law, including the Public Audit Act, Act No. 25 of 2004.

8.3.4 RESPONSIBILITIES OF EXTERNAL AUDIT

The responsibilities of Auditor General (AG) are outlined in the Public Audit Act. As external auditors, the Auditor General 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:

8.3.4.1 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;

8.3.4.2 DRDAR's compliance with any applicable legislation relating to financial matters, financial management and other related matters; and

8.3.4.3 The reported information relating to the performance of the department against predetermined objectives.

8.4 RISK MANAGEMENT OVERSIGHT

DRDAR's oversight framework on risk management is made up of the following structures:

- a. Risk Management Committee;
- b. Audit Committee;
- c. Accounting Officer; and
- d. Executive Authority

8.4.1 STRATEGIC VALUE OF RISK MANAGEMENT COMMITTEE

The Risk Management Committee is a governance structure appointed by the Accounting Officer. It is established to assist in designing, implementing and coordinating risk management activities within DRDAR. The responsibilities of the Risk Management Committee must be formally defined in the Risk Management Committee Charter or Terms of Reference (TORs).

8.4.2 RESPONSIBILITIES OF THE RISK MANAGEMENT COMMITTEE

8.4.2.1 The responsibilities of the Risk Management Committee include reviewing and recommending for approval the:

8.4.2.1.1 Enterprise Risk Management Framework and Policy;

8.4.2.1.2 Enterprise Risk Management Strategy;

8.4.2.1.3 Any material findings and recommendations by the assurance providers;

8.4.2.1.4 Risk Management Implementation Plan;

8.4.2.1.5 Incidents resulting from failed internal control measures affecting business continuity and the health or safety of officials;

8.4.2.2 Evaluation of the effectiveness of mitigating strategies to address material risks.

8.4.3 STRATEGIC VALUE OF THE AUDIT COMMITTEE

The responsibilities of the Audit Committee with respect to risk management shall be formally defined in its Charter. The Audit Committee is responsible for oversight of the department's control, governance and risk management. Furthermore the Audit Committee shall provide the Accounting Officer with independent counsel, advice and direction in respect of risk management.

8.4.4 RESPONSIBILITIES OF THE AUDIT COMMITTEE

8.4.4.1 The Audit Committee must provide an independent objective view of the effectiveness of Department's risk management;

8.4.4.2 The responsibilities of the Audit Committee include ensuring the Internal Audit and External Audit Plans are aligned to the Risk Profile of the Department;

8.4.4.3 Satisfy itself that it has appropriately addressed the following areas:

8.4.4.3.1.1 Financial reporting risks, including the risk of fraud;

8.4.4.3.1.2 Internal financial controls; and

8.4.4.3.1.3 IT risks as they relate to financial reporting.

8.4.4.4 Evaluate the effectiveness of Internal Audit in its responsibilities for risk management.

8.4.5 STRATEGIC VALUE OF THE ACCOUNTING OFFICER

The ultimate responsibility for the whole process of risk management lies with the Accounting Officer who must ensure that the responsibility of risk management is delegated to all levels of management and to all employees.

By setting the "tone at the top" the Accounting Officer promotes accountability and integrity and it ensures that risk management is integrated into all strategic management processes and that all significant risks are addressed.

8.4.6 RESPONSIBILITIES OF THE ACCOUNTING OFFICER

- 8.4.6.1 Delegating responsibilities for risk management to management and formation of internal structures such as Risk Management Committee and other governance committees;
- 8.4.6.2 Holding management accountable for designing, implementing, and monitoring and integrating risk management into their day-to-day activities.
- 8.4.6.3 Holding the internal structures accountable for performance in terms of their responsibilities for risk management;
- 8.4.6.4 Providing leadership and guidance to enable management and internal structures responsible for various aspects of risk management to properly perform their functions;
- 8.4.6.5 Ensuring that the control environment supports the effective functioning of risk management as discussed in paragraph 6.1 in the ERM Framework and Policy;
- 8.4.6.6 Approving the Risk Management Policy, Risk Management Strategy and Implementation Plan;
- 8.4.6.7 Approving the Department's risk appetite and risk tolerance and other policy related documents;
- 8.4.6.8 Devoting personal attention to overseeing management of significant risks;
- 8.4.6.9 Leveraging the Audit Committee, Internal Audit, External Audit and Risk Management Committee for assurance of risk management;
- 8.4.6.10 Ensuring appropriate action in respect of the recommendations of the Audit Committee, Internal Audit, External Audit and Risk Management Committee to improve risk management;
- 8.4.6.11 Providing assurance to relevant stakeholders that key risks are properly identified, assessed and mitigated.

8.4.7 STRATEGIC VALUE OF EXECUTIVE AUTHORITY

The Executive Authority is accountable to the legislature in terms of the achievement of goals and objectives of DRDAR. The Executive Authority shall take an interest in risk management to the extent necessary to obtain comfort that properly established and functioning systems of risk management are in place to protect the department against significant risks. As risk management is an important tool to support the achievement of this goal, the Executive Authority shall provide oversight on governance and risk management within DRDAR.

8.4.8 RESPONSIBILITIES OF EXECUTIVE AUTHORITY

- 8.4.8.1 Ensuring that the departmental strategies are aligned to its mandate;
- 8.4.8.2 Obtaining assurance from management that the department's strategic choices were based on a rigorous assessment of risk;
- 8.4.8.3 Obtaining assurance that key risks inherent in the department's strategies were identified and assessed, and are being properly managed;

- 8.4.8.4 Assisting the Accounting Officer to deal with fiscal, intergovernmental, political and other risks beyond their direct control and influence;
- 8.4.8.5 Insist on the achievement of objectives, effective performance management and value for money.

9. RECOMMENDATIONS AND APPROVAL



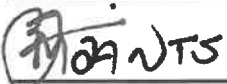
SAMELA SILI, Ms
CHIEF RISK OFFICER
DATE: 16 May 2023

Recommended/~~Not Recommended~~:



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

Recommended/~~Not Recommended~~:



SIBONGILE MZANTSI
DEPUTY DIRECTOR GENERAL – ADMINISTRATION (ACTING)
DATE: 30/05/2023

Approved/Not Approved



SIPHOKAZI NDUDANE
HEAD OF DEPARTMENT: DRDAR
DATE: 30/05/23