



health

Department:
Health
North West Provincial Government
REPUBLIC OF SOUTH AFRICA



2nd Floor, Health Office Park
Private Bag X 2068
MMABATHO
2735

**RISK & ETHICS
MANAGEMENT**

Tel: +27 (18) 391 4546
Email: sndou@nwpg.gov.za
www.health.nwpg.gov.za

Healthy self-reliant communities in the North West Province

RISK MANAGEMENT STRATEGY 2023/24

Author	Directorate: Risk and Ethics Management
Implementation Date	01 April 2023
Review Date	31 March 2024
Description	This document defines the Department's position on Risk Management Strategy

TABLE OF CONTENTS

MEANING OF ACRONYMS AND GLOSSARY TERMS	3
2. PURPOSE.....	6
3. LEGISLATIVE MANDATE	6
4. RATIONALE	6
5. STRATEGIC GOALS OF THE RISK MANAGEMENT FUNCTION.....	7
6 PLAN OF ACTION TO IMPROVE RISK MANAGEMENT MATURITY	7
6.1 Risk Culture Imbedding	7
6.2 Risk Identification and Assessment Methodologies.....	8
6.3 Risk Register	9
6.4 Risk Responses / Treatment plans.....	10
6.5 Monitoring	11
6.6 Reporting	11
6.7 Roles and Responsibilities.....	12
6.8 Anti-Fraud and Corruption.....	12
6.9 Ethics Management	12
6.10 Risk Management plan.....	12
7 RISK MODEL.....	13
7.1 Definition of risk categories.....	13
7.2 Likelihood and Impact Definitions	16
7.3 Impact Definitions and Tolerance Level.....	16
7.4 Impact and Likelihood Tables.....	16
8 RISK MANAGEMENT ACTIVITIES/ IMPLEMENTATION PLAN	19



MEANING OF ACRONYMS AND GLOSSARY TERMS

MEANINGS OF ACRONYMS	
Chief Financial Officer	CFO
Departmental Management Committee	DMC
Enterprise Risk Management	ERM
Information Communication Technology	ICT
Public Finance Management Act	PFMA
Public Sector Risk Management Framework of 2010	PSRMF
Risk Management Committee	RMC

GLOSSARY TERMS

Accounting Officer	Means the Head of the Department of Health
Action Owner	All officials of the department except for the chief risk officer and officials reporting to him/ her.
Chief Risk Officer	A senior official who is the head of the risk management unit
Control	An existing process, policy, device, practice or other action that acts to minimize negative risk or enhance positive opportunities.
Department	Refers to the department of Health
Impact	How the occurrence of the risk will affect the achievement of the set objective.
Inherent risk	A risk before taking into consideration the effect of applicable controls.



Likelihood	A general description of probability of the occurrence of an event
Modality	The way or mode in which something exists or is done
Monitor	To check, supervise, observe critically or measure the progress of an activity, action or system on a regular basis in order to identify change from the performance level required or expected.
Residual risk	Risk remaining after implementation of risk treatment.
Risk	Unwanted outcome, actual or potential, to the Institution's service delivery and other performance objectives, caused by the presence of risk factor/s. Some risk factor/s also present upside potential, which Management must be aware of and be prepared to exploit. This definition of "risk" also encompasses such opportunities.
Risk Appetite	The amount of residual risk that the Institution is willing to accept
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation.
Risk Capacity	Refers to how much risk an organization is able to take with respect to its resource and capabilities.
Risk Identification	Identification of threats to achievement of goals and objectives
Risk occurrence	The process of determining what, where, when, why and how something could happen.
Risk Owner	The person accountable for managing a particular risk
Risk Rating	Is a process whereby risks are evaluated to check whether they are high, medium or low by allocating numbers as indicated on the risk management strategy
Risk Tolerance	The amount of risk the Institution is capable of bearing(as opposed to the amount of risk it is willing to bear)

Risk treatment	A process of selection and implementation of measures to modify risk. Risk treatment measures can include avoiding, modifying, sharing or retaining risk.
-----------------------	---



2. PURPOSE

- 2.1 The purpose of the risk management strategy is to enable the Department of Health to implement the risk management policy.

3. LEGISLATIVE MANDATE

- 3.1 In terms of PFMA (section 38(1)(a)(i) the Accounting Officer for a department must ensure that the department has and maintains effective, efficient and transparent systems of financial, risk management and internal control.
- 3.2 Paragraph 3.2.1 of Treasury Regulations 2005, The Accounting Officer must also ensure that a Risk assessment is conducted regularly to identify emerging risks of the institution. The Risk Management strategy which must include Fraud prevention plan must be used to direct Internal Audit effort and priority, and to determine the skilled required of managers and staff to improve controls and to management Risk

4. RATIONALE

- 4.1 The setting of clear goals during the planning processes gives the organisation a clear picture of what needs to be achieved and also helps the organisation to objectively assess its current state and future/ desired state. As a matter of fact, risk management processes cannot be employed effectively where goals are not set or where objectives are ambiguous.
- 4.2 In an attempt to continuously improve the risk management processes, the Unit has deemed it fit to review its risk management strategy aligning it to the processes mentioned above on an annual basis focusing on

areas that are pertinent to the implementation and roll out of the overall departmental risk management strategy.

- 4.3 This will ensure that risk management processes remain in line with organisational changes that might be taking place and that all emerging risks can be identified and addressed promptly. As such the Department should see a change in mitigation of risks and yield some good results by appropriately implementing risk management principles

5. STRATEGIC GOALS OF THE RISK MANAGEMENT FUNCTION

- 5.1 The role or function of Risk Management is to develop and facilitate the implementation of effective risk management processes.
- 5.2 The goal is to ensure that effective risk management provides assurance to management in mitigating the identified risks and minimize the operational surprises and have organization free from risks, fraud and corruption.

6 PLAN OF ACTION TO IMPROVE RISK MANAGEMENT MATURITY

6.1 Risk Culture Imbedding

- 6.1.1 The Department currently exhibits a mixed risk culture with pockets of excellence seen in different some areas and at different levels. All the levels of maturity (according to Active risk ERM readiness guide 1) are seen in the Department and these are as follows;
 - a) There are those employees who have little awareness of risk management and its importance
 - b) There are also those employees who have heard about risk management but still regard it as an add-on function or a lost function like many other functions



- c) There are those who feel and acknowledge the importance of risk management but regard it as the risk officers' responsibility
- d) There are those who acknowledge the importance and want to participate but feel that there is no easier way to do risk management.
- e) There are those who have gotten to a point where risk management is now an intrinsic part of their processes though these are very few.

6.1.2 In order to attain uniformity in the embedding of the risk culture and working towards risk management becoming an intrinsic part of management and employees as well as creating a learning platform necessary for risk culture imbedding, depending on the capacity the Unit may do the following:

- a) Annual risk perception surveys
- b) Development and roll out of risk management capacitation plan for the Accounting officer, Management and Risk Management Committee,
- c) Conducting of internal risk workshops and awareness campaigns
- d) Induction workshops for all departmental committees on risk management issues pertaining to their area of focus

6.2 Risk Identification and Assessment Methodologies

6.2.1 The method used for risk identification will not overly rely on judgment techniques but rather draw as much as possible on unbiased independent sources including but not limited to:

- a) Internal and external audit reports
- b) Annual/Quarterly/Monthly Financial Statements or reports
- c) Data on actual losses
- d) Key performance information reports
- e) Data on peer groups
- f) Departmental Standard Operating Procedures



- 6.2.2 Root cause analysis will be conducted during the risk identification process to ensure relevance of identified risks as well as the root causes.
- 6.2.3 The assessment / voting process shall adequately assess consequences and root causes giving rise to each risk, a score or risk rating.
- 6.2.4 The risk shall be assessed in terms of *likelihood* and *Impact* of the risk occurring.
- 6.2.5 These assessment shall be rated on a scale of 1-5, where 1 is low, mostly acceptable- low level of control intervention required and 5 is maximum, unacceptable- action must be taken immediately.
- 6.2.6 The methodologies will be applicable to all areas of risk assessments including strategic and operational risk assessments.
- 6.2.7 The project risk assessments will be conducted during the Annual Operational Risk Assessments.
- 6.2.8 Annual Strategic Risk Assessment exercise shall run concurrently with the strategic planning session to ensure a successful risk management practices and process within a department.

6.3 Risk Register

- 6.3.1 Department risk registers should be a “live document”, not a tick-box approach, and must not become bureaucratic.
- 6.3.2 The department shall conduct a formalized risk assessment at least annually. The assessment will include the identification, measurement and categorization of all key risks that could potentially affect the strategic and operational objectives as well as projects of

the department so as to develop and manage **Strategic and Operational risk registers**

6.3.3 Once basic information on each risk is collected, the Risk Management Committee and the Departmental Management Committee shall only require to be notified of key changes since the last update

6.4 Risk Responses / Treatment plans

6.4.1 This is the stage of risk management where one has taken a decision to treat the risk. Treatment plans refer to implementation of mitigating strategies to ensure that risks are minimised to an acceptable level. The process involves selections of adequate mitigation strategies which will reduce or eliminate the level of the residual risk. In responding to the risks identified, the following responses shall be considered

6.4.2 Risk Treatment, - Risk Owners and Management shall ensure that immediate adequate interventions through series of actions are implemented to ensure an acceptable level of residual risk.

6.4.3 Risk Transfer, - Risk Owners and Management shall ensure that an adequate transfer of risk through a third party by way of outsourcing some of our services takes place effectively and efficiently.

6.4.4 Risk Tolerance, - Risk Owners and Management shall tolerate some of the risks as prescribed in this policy. Furthermore, management must also monitor the risk to ensure that its likelihood and impact does not change. If the residual risk becomes high



management must ensure that appropriate action is taken to ensure that the risk is treated.

6.4.5 Risk Termination - Risk Owners and Management shall terminate the risk through quick and decisive action to eliminate the risk altogether

6.5 Monitoring

6.5.1 Monitoring shall be done quarterly for the strategic register and monthly for operational registers on the key risks, and mitigation strategies by risk owners.

6.5.2 Risk Management unit shall also provide guidance as far as is necessary to all Risk owners.

6.5.3 Residual risk re-rating will be done on a quarterly basis for both Strategic risk and operational risks.

6.6 Reporting

6.6.1 The Risk Management Unit shall formally set reporting measures on a Risk register for compliance to monitor movement trends and risk progress, those shall be as follows:

- a) Operational risk mitigations reporting shall be done by Risk Owners on monthly basis.
- b) Strategic Risk mitigations reporting shall be done by Action Owners on quarterly basis.

6.6.2 Quarterly risk reports shall be presented together with other feedback reports following the quarterly departmental district and provincial reviews to Risk Management Committee.

6.6.3 The quarterly risk reports, APP Performance Reports and other assurance reports from PIA and Auditor General will form the basis from which emerging risks may be identified.

6.6.4 Risk Management shall be a standing agenda item at Departmental Management Committee (DMC) meetings to ensure consistent and on-going monitoring and reporting.

6.7 ROLES AND RESPONSIBILITIES

6.7.1 Every employee has a role to play in executing risk management processes and adhering to risk management procedures laid down by NWDoH in their areas of responsibilities.

6.7.2 Roles and responsibilities are outlined in section 6 of Departmental Risk Management policy

6.8 Anti-Fraud and Corruption

6.8.1 Anti-fraud and Corruption Strategy will be dealt with in a separate policy "Anti-fraud and Corruption Policy" and the strategy thereof.

6.9 Ethics Management

6.9.1 Ethics Management will be dealt with in separate policy, "Policy on Ethics and Code of Ethical Conduct" and the strategy thereof.

6.10 Risk Management plan

6.10.1 Risk management plan will provide the roll-out plan of all the activities. That plan is included in the Risk Management Strategy document.



7 RISK MODEL

Risk modality shall be as follows:

7.1 Definition of risk categories

Each risk (Strategic and Operational) should be rated and categorized in terms of the impact the risk may have and should be in line with the below.

Risk Category	Description
Human Resource	Risks affecting the Department's Human Resource with regard to : Integrity & Honesty -Recruitment -Skills & Competence -Employee Wellness -Employee Relations -Retention -Occupational Health & Safety
Knowledge & Information Management	Risks relating to a the Department's management of knowledge and information regarding the following: -Availability of information -Stability of information -Integrity of information -Relevance of information -Retention of information -Safeguarding of information
Litigation	Risk that the Department will suffer losses due to litigation and claims from: -Claims by employees, public, service providers and other third parties -Failure by the Department to exercise certain rights that are to its advantage

Loss/Theft of Assets	Risks that the Department might suffer losses due to either theft or loss of its assets
Material Resources (Procurement Risks)	Risks relating to the Department's material resources with regard to: -Availability of material -Costs & means of acquiring resources -Wastage of material resources
Service Delivery	Risk that the Department will not deliver the appropriate quality of service to its stakeholders
Information Technology	Risks relating to the Department's IT objectives with consideration for the following: -Security Concerns -System Uptime -Applicability of IT infrastructure -Integration of Systems (interface) -Effectiveness of Technology -Obsolescence of Technology
Health & Safety	Risks from occupational Health & Safety issues such as: -Injury on Duty Outbreak of Disease in the Department
Disaster Recovery/ Business Continuity	Risks relating to the Department's preparedness to disasters that could impact the normal functioning of the Department, e.g. -Natural Disasters -Acts of Terrorism
Compliance/ Regulatory	Risks related to the compliance requirements that the Department must meet, including: -Failure to monitor or enforce compliance

	<ul style="list-style-type: none"> -Monitoring and enforcement mechanisms -Consequences of Non-Compliance -Fines & Penalties paid
Fraud & Corruption	Risks relating to illegal or improper acts by Department's officials resulting in a loss to the Department or others
Financial	<p>Risks encompassing the entire scope of general financial management, including:</p> <ul style="list-style-type: none"> -Cash Flow adequacy and management thereof -Financial Losses -Wasteful expenditure -Budget Allocation -Financial Statement Integrity -Revenue Collection -Increasing Operational Expenditure
Reputational	Risks and other factors that could tarnish the Department's reputation, public perception and image
Economic Environment	<p>Risks relating to the Department's economic environment including:</p> <ul style="list-style-type: none"> -Inflation -Foreign exchange fluctuation -Interest rates
Political Environment	<p>Risks that arise from political factors and decisions that have an impact on the Department's mandate and operations, including:</p> <ul style="list-style-type: none"> -Political Unrest -Political interference -Local, Provincial and National elections -Changes in Political Office bearers

7.2 Likelihood and Impact Definitions

Each risk should be rated in terms of the likelihood of the risk occurring as per the guidelines provided below. The likelihood ratings are consistent for Strategic & Operational Risks.

7.3 Impact Definitions and Tolerance Level

The below tables indicates the acceptable level of tolerance per residual risk assessed

7.4 Impact and Likelihood Tables

7.4.1 Rating table to assess the Impact and Likelihood of risks

The below table is used to assess the impact and acceptable level of tolerance per residual risk assessed:-

Rating	Assessment	Definition
1	Insignificant	There is a 90%-100% chance that the objective will certainly be achieved. (Acceptable - No action required)
2	Minor	There is a 70%-89% likelihood of the objective being achieved. (Mostly acceptable - Low level of control intervention required, if any)
3	Moderate	There are 50%-69% chances that it is likely that the objective will be achieved. (Moderate level of control intervention required)
4	Major	There is a 30%-49% chance that the objective will be achieved. (Unacceptable level of risk - Major level of control intervention required)
5	Critical	There is 1-29% likelihood that the objective will be achieved. (Unacceptable- Action must be taken immediately)



7.4.2 Rating table to assess the likelihood of risks

The below table is used to assess the likelihood of risk occurring

Rating	Assessment	Definition
1	Rare	The risk is conceivable but is only likely to occur in extreme circumstances
2	Unlikely	The risk occurs infrequently and is unlikely to occur within the next 12 months
3	Moderate	There is an above average chance that the risk will occur at least once in the next 12 months
4	Likely	The risk could easily occur, and is likely to occur at least once within the next 12 months
5	Common	The risk is already occurring, or is likely to occur more than once within the next 12 months

7.4.3 Rating table, Inherent risk exposure (impact x likelihood): Residual risk exposure (inherent risk x control effectiveness)

The table below shows the required action in relation to each risk rating level, this table is used when treatment plans were developed. However, certain environmental factors such as Supply chain process and Human Resources Processed are also considered

Risk rating	Risk magnitude	Response
20 - 25	Maximum	Unacceptable- Action must be taken immediately(0-3 months)
15 - 19	High	Unacceptable level of risk, except under unique circumstances or conditions - Major level of control intervention required to achieve an acceptable level of residual risk (3-6 Months)
10 - 14	Medium	Unacceptable level of risk, except under unique circumstances or conditions - Moderate level of control intervention required to achieve an acceptable level of residual risk (6-12 Months)
5 - 9	Minimum	Mostly acceptable - Keep routine control procedures in check
1 - 4	Low	Acceptable-keep routine control procedures in check

7.4.4 Impact and likelihood

The following is a rating table used to categorize the various levels of inherent and residual risk.

LIKELIHOOD	5	Common	5	10	15	20	25
	4	Likely	4	8	12	16	20
	3	Moderate	3	6	9	12	15
	2	Unlikely	2	4	6	8	10
	1	Rare	1	2	3	4	5
			Insignificant	Minor	Moderate	Major	Critical
	Rating		1	2	3	4	5
	IMPACT						

8 RISK MANAGEMENT ACTIVITIES/ IMPLEMENTATION PLAN

8.1 The aim of the implementation plan is to give an outline of how all the strategies stated in this document will be rolled out as a way of steering the department in the desired direction that gives reasonable assurance that the goals set for this year and subsequent years will be achieved.

8.2 The detailed plan is attached as Annexure A.

9. Approval

RECOMMENDED:



MR. L.A GOPANE
CHAIRPERSON RMC
DEPARTMENT OF HEALTH

31/01/2023
DATE

APPROVED



MR. O.E. MONGALE
SUPERINTENDENT GENERAL
DEPARTMENT OF HEALTH

31/01/2023
DATE

Annexure A

RISK MANAGEMENT ACTIVITIES/ IMPLEMENTATION PLAN 2023/2024

KEY PERFORMANCE INDICATORS (KPI)	ACTIVITY/ ACTION	PLANNED	RESPONSIBLE PERSONS	DUE DATE	OUTPUTS/OUTCOMES	PROGRESS	REASON FOR DEVIATION /COMMENT
RISK PROFILE							
Development of Risk Management Implementation Plan for 2023/2024	Development of the Risk Management Implementation Plan	the CRO		31 March 2023	Approved Management Implementation Plan		
ENABLING DOCUMENTS							
Review Management enabling documents for 2023/2024	1. Tabling the documents to the Risk Management Committee (RMC).	CRO	RMC	31 March 2024	a. Approved Risk Management Policy b. Approved Risk Management Strategy		

	<p>2. Review and adoption of the documents by the RMC</p> <p>3. Submission to Accounting Officer.</p>	CRO		<p>c. Approved Risk Management Committee Charter</p> <p>d. Approved Risk Management Committee KPI</p>	
ASSESSMENTS					
<p>Conduct annual Risk Assessments and ensure availability of Risk Registers</p>	<p>1. Conduct strategic risk assessment</p> <p>2. Compile Strategic Risk Register</p>	CRO and SMS	31 March 2023	<p>a. Final Draft Strategic Risk Register.</p> <p>b. Attendance Registers</p>	
		CRO	31 March 2023	<p>a. Strategic Assessment Report.</p> <p>b. Approved Strategic Risk Register 2022/23</p>	

	3. Conduct operational risk assessments	CRO	30 June 2023	a. 2023/24 Consolidated Operational Risk Register b. Approved Operational Risk Assessment Tools		
MONITORING						
Monitoring risk management and activities within the Department.	1. Table progress Report on Strategic Risks	CRO	Quarterly	Strategic risk monitoring progress report		
	2. Assessment of the Report & Recommendation to the Accounting Officer.	RMC		Approved Management Report	Risk Committee	
	3. Table progress Report on Operational Risks	CRO	2 nd , 3 rd , 4 th Quarter	Operational risk monitoring progress report.		
	4. Assessment of the Report & Recommendation to the Accounting Officer.	RMC	Approved Management Report	Risk Committee		

CAPACITY BUILDING

Facilitate the capacity building Programme on risk management	Training of Members Management	RMC and	CRO	Annually	Attendance Register	
---	--------------------------------	---------	-----	----------	---------------------	--

RISK MANAGEMENT COMMITTEE REPORTS

Submission of Quarterly Reports to the Accounting Officer.	Endorsing the tabled Risk Management Reports by CRO	RMC	Quarterly	Approved Management Report	Risk Committee	
--	---	-----	-----------	----------------------------	----------------	--



 MR. L.A GOPANE

**INDEPENDENT CHAIRPERSON
 RISK MANAGEMENT COMMITTEE**



 MR. O.E. MONGALE

**SUPERINTENDENT GENERAL
 DEPARTMENT OF HEALTH**

3/10/2023
 DATE

31/01/2023
 DATE

