

OFFICE OF THE PREMIER

RISK MANAGEMENT STRATEGY

FOR 2025/2026 FINANCIAL YEAR

Table of Contents

1.	INTRODUCTION	3
2.	PURPOSE	3
3.	DEFINITION OF A RISK	3
4.	DEFINITION OF RISK MANAGEMENT.....	4
5.	LEGAL MANDATE.....	4
6.	APPLICATION.....	5
7.	PREVENTION OF FRAUD AND CORRUPTION.....	5
8.	CORPORATE GOVERNANCE OF INFORMATION AND COMMUNICATION TECHNOLGY.....	6
9.	RISK MANAGEMENT PROCESS	7
9.6.1	GOVERNANCE AND CULTURE.....	8
9.6.2	STRATEGY AND OBJECTIVE-SETTING	8
9.6.3	PERFORMANCE	8
9.6.4	REVIEW AND REVISION	9
9.6.5	MANAGEMENT OF EMERGING RISKS\.....	9
10.	RISK MANAGEMENT COMMITTEE	13
11.	ROLES AND RESPONSIBILITIES	13
12.	RISK MANAGEMENT STRUCTURE.....	25
13.	REVIEW.....	26
14.	RISK MANAGEMENT IMPLEMENTATION PLAN.....	26
14.1	OBJECTIVE.....	26
14.2	APPROACH	26
14.3	DETAILED RISK MANAGEMENT IMPLEMENTATION PLAN.....	26

1. INTRODUCTION

- 1.1 The Risk Management Strategy outlines a high-level plan on how the Office will go about implementing its Risk Management Policy. It is informed by the Risk Management Policy and the risk profile of the Office. A risk profile with a high level of threat to objectives will require a more rigorous commitment to risk management.
- 1.2 It describes the Office of the Premier's risk management and sets out the requirements for management in generating risk management action plans that will ensure that the Office performs its strategic role of monitoring and evaluation at an optimum level.
- 1.3 It is also important to indicate that this strategy will assist the Office to attain its strategic objectives and programmes to better the service delivery.

2. PURPOSE

- 2.1 The Purpose of this strategy is to enable the Office of the Premier to comply with legal requirements relating to risk management and to demonstrate adherence to good governance, while at the same time enhancing operations required for the achievement of the strategic objectives of the Office.

3. DEFINITION OF A RISK

- 3.1 Risk is defined consistent with Chapter 1 of the North West Provincial Risk Management Framework an unwanted outcome, actual or potential, to the Institution's service delivery and other performance objectives, caused by the presence of risk factors (s). Some risk factor(s) also present upside potential, which Management must be aware of and must be prepared to exploit. This definition of "risk" also encompasses such opportunities.

CONFIDENTIAL

- 3.2 Corporate Governance of Information and Communication risks are those risks that may have a negative impact on evaluating and directing the use of the information and communication technology to support the organization and monitoring this use to achieve strategic objectives of the Office.

4. DEFINITION OF RISK MANAGEMENT

- 4.1 Risk Management is a continuous, proactive, systematic and formalized process effected by Executive Authority, Accounting Officer, management and other personnel, applied in strategic planning and across the Office, designed to identify potential events that may affect the Office, and manage risks to be within its tolerance, to provide reasonable assurance regarding the attainment of objectives of the Office.

5. LEGAL MANDATE

- 5.1 The strategy is based on the requirements of the Public Finance Management Act (PFMA), Treasury regulations and North West Provincial Risk Management Framework.
- 5.2 Section 38(1)(a)(i) of the Public Finance Management Act requires that “an Accounting Officer for a department must ensure that the department has and maintains effective, efficient and transparent system of finance, risk and internal control”
- 5.3 The extension of the general responsibilities, in term of section 45 of the PFMA, to other officials is cornerstone in the institutionalization of risk management in the Public Service. It establishes responsibility for risk management at all levels of management, extending it beyond the roles of the Accounting Officer in this regard.
- 5.4 Paragraph 3.2.1. of Treasury regulations requires that “an Accounting Officer for a department must ensure that a risk assessment is conducted regularly to identify emerging risk of the Institution. A risk Management Strategy, which must include

CONFIDENTIAL

a fraud prevention plan, must be used to direct internal audit effort and priority, and to determine the skills required of managers and staff to improve controls and to manage these risks. The strategy must be clearly communicated to all officials to ensure that the risk management strategy is incorporated into the language and culture of the institution”.

5.5 The Committee of Sponsoring Organizations (COSO) Enterprise Wide Risk Management framework updated in June 2017 stipulating principles organized into five interrelated components namely: Governance & culture, Strategy & objective setting, Performance, Review & revision, and Information, Communication and Reporting.

5.6 Corporate Governance of Information and Communication Technology Policy framework requires that the Risk Management Policy of the Office include how business –related ICT risks will be managed and how capacity will be created in the Risk Management function to address ICT related risks.

In compliance with the requirements alluded to above, Office of the Premier intends to apply a consistent framework for the management of risk. This shall incorporate the application of the risk management strategy, processes, plans and infrastructure.

6. APPLICATION

6.1 The application of this strategy will be the responsibility of the Accounting Officer, through the organizational management structure. Management at all levels is responsible for the implementation of this strategy.

7. PREVENTION OF FRAUD AND CORRUPTION

7.1 Office of the Premier perceives fraud and corruption as an obstacle to provide quality service delivery.

CONFIDENTIAL

- 7.2 Fraud and Corruption investigations shall be conducted internally by the appropriate governance structure or referred to external bodies per The Accounting Officers' discretion.
- 7.3 All suspected fraudulent activities should be reported to the Accounting Officer who will assess the incident and allocate it to the appropriate governance structure for full investigation.
- 7.4 It is therefore the responsibility of every employee to report incidents of fraud and corruption that may come to his/her attention through the whistle blow mechanism developed by the forensic management services.
- 7.5 Fraud and Corruption prevention strategy has been revised to accommodate mechanisms to deal with IT fraud risks and other fraud risks emanated from the new programmers of the Office.
- 7.6 The approved Fraud and Corruption Prevention Policy and Strategy will be communicated to all employees and stakeholders through forensic management services.

8. CORPORATE GOVERNANCE OF INFORMATION AND COMMUNICATION TECHNOLOGY

- 8.1 Office of the Premier will ensure that all three Phases of the implementation of Corporate Governance of Information and Communication Technology Policy Framework are attained through identifying, assessing and mitigating Corporate Governance of ICT risks that could prevent the Office from achieving the set targets as required by the DPSA.
- 8.2 Risk Management Unit will be capacitated with officials who have a thorough understanding of Corporate Governance of Information and Communication Technology policy framework policy and the implementation guideline.

9. RISK MANAGEMENT PROCESS

- 9.1. The Public Sector Risk Management Framework defines risk as 'an unwanted outcome, actual or potential, to the department's service delivery or other performance objectives, caused by the presence of risk factors.'
- 9.2. From the above definition it follows that setting organizational goals and objectives brings about risk that such goals may not be attained. These risks have to be assessed and prioritized according to significance as it is believed that the Department will not have sufficient resources to adequately address all the risks it faces.
- 9.3. Control interventions are developed for all significant risks identified and monitored on a regular basis.
- 9.4. Enterprise Risk Management consists of a set of principles organised into five (5) interrelated components. These components are:
1. Governance and Culture:
 2. Strategy and Objective-Setting:
 3. Performance:
 4. Review and Revision
 5. Information, Communication, and Reporting
- 9.5. The five components are supported by a set of principles, adhering to these principles can provide management with a reasonable expectation that the organisation understands and strives to manage the risks associated with its strategy and business objectives.

9.6. The diagram below shows the process schematically.



9.6.1 Governance and Culture

- Governance sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. Culture pertains to ethical values, desired behaviors, and understanding of risk in the entity.

9.6.2 Strategy and Objective-Setting

- Enterprise risk management, strategy, and objective-setting work together in the strategic-planning process. A risk appetite is established and aligned with the strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.

9.6.3 Performance

- Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks are prioritized by severity in the context of risk appetite. The organization then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.

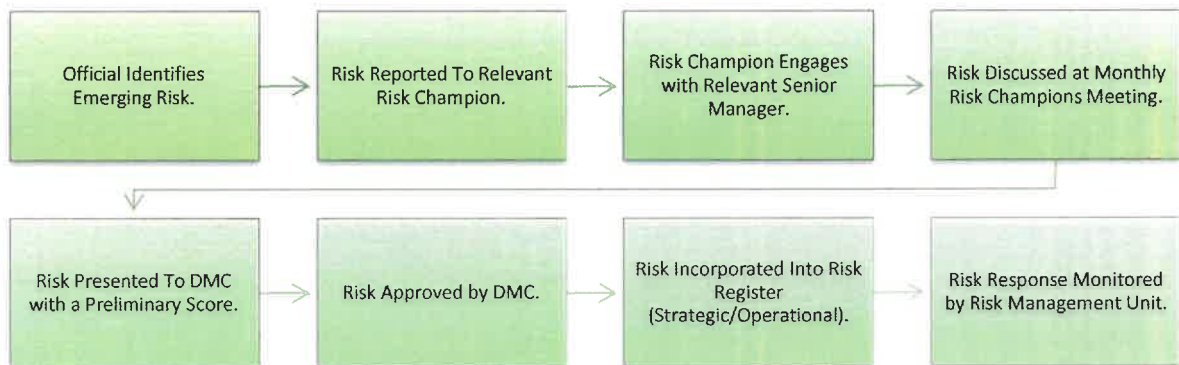
9.6.4 Review and Revision

- By reviewing entity performance, an organization can consider how well the enterprise risk management components are functioning over time and in light of substantial changes, and what revisions are needed.
- Risk identification at both strategic and operational level should be performed at least once a year.

9.6.5 Management of Emerging Risks\

- Since risk is dynamic by nature, the Department has outlined a process to ensure that emerging risks are identified and systematically managed. Risk Management Champions will act as the link between officials and the risk management unit in the management of emerging risks.

9.7. This process is depicted below in diagram format:



9.7.1 Risk assessment assists the Department to prioritize and direct efforts to the most important risks. The Public Sector Risk Management Framework defines risk

CONFIDENTIAL

assessment as *“a systematic process to quantify and quality the level of risk associated with a specific event or threat”*

9.7.2 Identified risks will be assessed on the likelihood of the occurrence of a threat or event and impact of such threat or event on the achievement of the Department's objectives.

9.7.3 The Department complies with the requirements of the Public Sector Risk Management Framework which determines that risks be assessed in three (3) stages:

I. Inherent Risk

The concept of inherent risk refers to the level of risk exposure faced by Department in the absence of deliberate management actions (controls) to mitigate the risk.

II. Residual Risk

Residual risk refers to actual level of risk exposure faced by the Department after taking into account the effects of management's efforts to mitigate the risk.

III. Residual Risk Benchmarking

Residual risk should be measured against the Department's risk tolerance level to determine whether there is a need for further management efforts to mitigate such risks.

9.7.4 Identified risks should be expressed in the same unit of measure used for the Key Performance Indicator(s) concerned.

9.7.5 Risk assessment will be re-performed for all key risks should significant changes be noted in the environment within which the Department operates. To ascertain whether a shift in the magnitude of risk has taken place and whether further

CONFIDENTIAL

management effort is warranted, risk assessment will be performed at least once a year.

Risk Assessment Impact Rating Matrix

The following is a rating table used to assess the potential impact of risks.

Rating	Assessment	Definition
1	Insignificant	Acceptable – No action required for objective to be achieved.
2	Minor	Mostly acceptable - Low level of control intervention required to achieve the objective.
3	Moderate	Moderate level of control intervention required to achieve the objective.
4	Major	Unacceptable level of risk - Major level of control intervention required to achieve the objective
5	Critical	Unacceptable- Action must be taken immediately to achieve the objective.

Risk Assessment Likelihood Rating Matrix

The following is a rating table used to assess the likelihood of risks.

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

CONFIDENTIAL

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

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

The table below shows the required action in relation to each risk rating level; this table will be considered when risk treatment plans are developed.

Risk Score	Rating	Action	Response Time
1-4	Very Low	Acceptable - No action required	NA
5-9	Low	Broadly acceptable – Keep routine control procedures in check	NA
10-14	Medium	Moderate - reduce risks in medium-term.	6 – 12 Months
15-19	High	High Risk - priority action to be undertaken in short-term.	3 – 6 Months
20-25	Very High	Unacceptable -action must be taken IMMEDIATELY.	0 – 3 Months

10. RISK MANAGEMENT COMMITTEE

10.1 A Risk Management Committee shall be appointed by the Accounting Officer to assist him/her in discharging risk management and control responsibilities in accordance with PFMA no. 1 of 1999, Section 38 (a) in respect of ***“general responsibilities of the Accounting Officer”*** and Chapter 11, Section 22 of the North West Provincial Risk Management Framework on ***“functions of the Accounting Officer / Authority with respect to risk management”***.

10.2 The membership of the Risk Management Committee shall comprise both Management and external members with the necessary blend of skills, competencies and attributes, including following critical aspects:

- an intimate understanding of the mandate and operations of the Office,
- the ability to act independently and objectively in the interest of the Office,
- thorough knowledge of risk management principles and their application.

10.3 The responsibilities of the Risk Management Committee shall be formally defined in a Charter approved by the Accounting Officer.

11. ROLES AND RESPONSIBILITIES

11.1 The following roles and responsibilities relate to the various committees and officials responsible for risk management within the Office of the Premier. The listed roles and responsibilities only relate to the risk management functions.

CONFIDENTIAL

	Responsibilities	Accountability	Frequency
Executive Authority			
1	Ensuring that the strategies of the Office are aligned to its government mandate.	EA	After every five years.
2	Obtaining assurance from Management that the strategic choices of the Office were based on assessment of risk.	EA	After Every five years
3	Obtaining assurance that key risks inherent in the strategies of the Office were identified, assessed, and are being properly managed.	EA	Quarterly
4.	Assisting the Accounting Officer to deal with fiscal, intergovernmental, political and other risks beyond the Accounting Officer direct of control and influence.	EA	Annually or when there is a re-configuration of the Office.
5.	Insisting on the achievement of objectives, effective performance management and value for money.	EA	Annually
6.	Requiring that management should establish set of values by which every employee should abide by.	EA	Ongoing

CONFIDENTIAL

	Responsibilities	Accountability	Frequency
Accounting Officer			
1.	Setting the tone at the top by supporting Enterprise Risk Management and allocating resources towards the implementation thereof	AO	Ongoing
2.	Approve the following: <ul style="list-style-type: none"> • Risk Management policy and strategy; • Risk Implementation Plans; • Fraud risk register; • Fraud risk implementation plan, • Risk Management Committee Charter. 	AO	Annually
3	Establishing the necessary structure and reporting lines within the Office to support Enterprise Risk Management.	AO	As and when required.
4.	Approving the risk appetite and risk tolerance of the Office.	AO	Continuous
5.	Influencing a risk awareness culture in the Office.	AO	Annually
6.	Approving the code of conduct for the Office and holding management and officials accountable towards risk management.	AO	Quarterly

CONFIDENTIAL

	Responsibilities	Accountability	Frequency
7.	Place the key risks at the forefront of the management agenda and devote personal attention to overseeing their effective management.	AO	Quarterly
8.	Hold management accountable for designing, implementing, monitoring and integrating risk management principles into their day-to day activities.	AO	Annually
9.	Holding the structures responsible for risk management activities accountable for adequate performance.	AO	Ongoing
10.	Ensuring that a conducive control environment exists to ensure that identified risks are proactively managed.	AO	Ongoing
11.	Provide all relevant stakeholders with the necessary assurance that key risks are properly identified, assessed, mitigated and monitored.	DRMC	As and when required.
12.	Consider and act on recommendations from the Audit Committee, Internal Audit, Risk Management Committee and other appropriate structures for improving the overall state of risk management.	DRMC	As and when the recommendations are made available.

CONFIDENTIAL

	Responsibilities	Accountability	Frequency
13.	Provide appropriate leadership and guidance to Senior Management and structures responsible for various aspects of risk management.	DMRC	Continuous
14.	Appoint members of the Risk Management Committee.	AO	Consistent with the NWPRMF (Chapter 13)
Risk Management Committee			
	Responsibilities	Accountability	Frequency
1.	Review and recommend for the approval of the Accounting Officer the following: <ul style="list-style-type: none"> • Risk Management Policy. • Risk Management Strategy. • Risk Management Implementation Plan. • Risk Management Champions charter. • Fraud Prevention Policy and Strategy, • Fraud Risk Implementation Plan. 	RMC	Annually
2.	Assess implementation of the Risk Management Policy, Strategy, Implementation Plan, Fraud Prevention Policy and Strategy and Fraud Prevention Implementation Plan.	RMC	Annually

CONFIDENTIAL

	Responsibilities	Accountability	Frequency
3	Review the risk identification and assessment methodologies of the Office to obtain reasonable assurance of the completeness and accuracy of the risk.	RMC	Annually
4.	Evaluate the effectiveness of mitigating strategies implemented to address the material risks of the Office of the Premier.	RMC.	Quarterly
5.	Report to the Accounting Officer any material changes to the risk profile of the Office of the Premier.	RMC	Quarterly
6.	Review any material findings and recommendations by assurance providers on the system of risk management and monitor the implementation of such recommendations.	RCM	Quarterly
7	Provide proper and timely reports to the Accounting Officer on the state of risk management, together with a committee's recommendations to address any deficiencies identified by the Committee.	RMC	Quarterly
8.	Develop its own key performance indicators for approval by the Accounting Officer.	RMC	After every two years.

CONFIDENTIAL

	Responsibilities	Accountability	Frequency
9.	Interact with the Audit Committee to share information relating to material risks of the Office.	RMC	Quarterly
10.	Develop/review Risk Management Committee Charter for an approval by the Accounting Officer.	RMC	Annually
Deputy Directors General			
	Responsibilities	Accountability	Frequency
1	Intervening in and escalating instances where risk management efforts are being hampered by the lack of cooperation by Management and other official by the lack of institutional skills and expertise.	Risk Champions	Continuous
2.	Assist the risk owners in their programmes to resolve risk related problems.	Risk Champions	Continuous
3.	Providing guidance and support to manage problematic risks and risks of a transversal nature that require a multiple participant approach.	Risk Champions	Continuous
Chief Financial Officer			
	Responsibilities	Accountability	Frequency

CONFIDENTIAL

	Responsibilities	Accountability	Frequency
1	Develop and implement a plan to integrate risk management into the day-to-day financial activities of the Office. (Internal Control Strategies)	Chief Financial Officer	Continuous
Chief Risk Officer			
	Responsibilities	Accountability	Frequency
1	Working with Senior Management to develop the Office's vision for risk management.	Chief Risk Officer/ Top Management	As and when required.
2	Developing and updating the following: <ul style="list-style-type: none"> • Risk Management Policy, • Risk Management Strategy. • Risk Implementation Plans. • Related risk management literature 	Chief Risk Officer	Annually
3	Developing in consultation with management inter alia, the: <ul style="list-style-type: none"> • Risk identification and assessment methodology; • Risk appetite and tolerance statements. 	Chief Risk Officer	On going
4.	Facilitating orientation and training for the Risk Management Committee and Secretarial services	Chief Risk Officer	On going

CONFIDENTIAL

	Responsibilities	Accountability	Frequency
6.	Continuously driving risk management to higher levels of maturity.	Chief Risk Officer	On going
7.	Assisting management with risk identification, assessment and development of response strategies.	Chief Risk Officer	On going
8.	Monitoring the implementation of the risk response strategies.	Chief Risk Officer	Continuous
9.	Compile risks reports for perusal and approval by the Risk Management Committee.	Chief Risk Officer	Continuous
10.	Analyze the results of the risk assessments.	Chief Risk Officer	Continuous
11.	Participating with internal audit, management and Auditor General in developing the combined assurance plan.	Chief Risk Officer	As and when required.

Level 13-14(Management)			
	Responsibilities	Accountability	Frequency
1.	Empowering officials to perform effectively in their risks management responsibilities through proper communication of responsibilities, comprehensive orientation and ongoing opportunities for skills development.	Level 13-14	On going

CONFIDENTIAL

Level 13-14(Management)			
	Responsibilities	Accountability	Frequency
2.	Aligning the functional risk management methodologies and processes with the Departmental process.	Level 13-14	On going
3	Devoting personal attention to overseeing the management of key risks within their area of responsibility.	Level 13-14	On going
4.	Maintaining a sound relationship with the Risk Management Unit and Risk Champions	Level 13-14	On going
5.	Analyse and consolidate risk management reports.	Level 13-14	Quarterly
6.	Present risk management reports to the Risk Management Committee.	Level 13-14	As and when required
7.	Maintaining the proper functioning of the control environment within their area of responsibility.	Level 13-14	Continuous
9.	Implementing the directives of the Accounting Officer concerning risk management.	Level 13- 14	Continuous
10.	Developing and implementing fraud risks response plan for their fraud risks	Level 13-14	Continuous
13.	Execute responsibilities in consultation with Strategic Management Unit.	Level 13-14	Continuous
Other Personnel			

CONFIDENTIAL

Level 13-14(Management)			
	Responsibilities	Accountability	Frequency
(Level 4 -12)			
	Responsibilities	Accountability	Frequency
1.	Familiarity with the overall enterprise risk management vision, Risk Management Policy and Strategy and Fraud Prevention Policy, Fraud Prevention Strategy.	Level 4-12	Continuous
2.	Applying the risk management process to their respective functions.	Level 4-12	Continuous
3.	Maintaining the functioning of the control environment, information and communication as well as the monitoring systems within their delegated responsibility.	Level 4-12	Continuous
4.	Participation in risk identification and risk assessment within their business unit.	Level 4-12	Continuous
5.	Adhering to the code of conduct of the Office.	Level 4-12	Continuous
6	Implementing the delegated action plans to address the identified risks	Level 4-12	Continuous
7.	Informing their supervisors and / or the Risk Management Unit of new risks and significant changes in known risks.	Level 4-12	Continuous

CONFIDENTIAL

Level 13-14(Management)			
	Responsibilities	Accountability	Frequency
8.	Co-operating with other role players in the risk management process and providing information as required.	Level 4-12	Continuous
9.	Reporting inefficient, unnecessary or unworkable controls to the Risk Management Unit.	Level 4- 12	Continuous
10.	Reporting suspicion of Fraud and Corruption to the Forensic Management Services	Level 4-12	Continuous
Audit Committee			
	Responsibilities	Accountability	Frequency
1.	Review the completeness of risk assessment process implemented by Management.	Audit Committee	Annually
2	Reviews the risk profile and management action plans to address the risks.	Audit Committee	Quarterly
3	Monitor the progress made with the management of action plan.	Audit Committee	Quarterly
4	Review the progress made with regards to the implementation of the risk management strategy	Audit Committee	Quarterly
5	Reviews and recommends any risks disclosures in the annual financial statements.	Audit Committee	Annually

CONFIDENTIAL

Level 13-14(Management)			
	Responsibilities	Accountability	Frequency
6	Provides regular feed back to the Accounting Officer on the effectiveness of the risk management.	Audit Committee	Quarterly
7.	Reviews and ensures that the internal audit plans are aligned to the risk profile of the Office of the Premier	Audit Committee	Annually
Internal Audit			
No	Responsibilities	Accountability	Frequency
1	Utilize risk assessment report to compile its strategic and coverage audit plans.	Internal Audit	Annually
2.	Formally review the effectiveness of the risk management processes.	Internal Audit	Annually

12. RISK MANAGEMENT STRUCTURE

12.1 For Risk Management to be integrated and effective within Office of the Premier the structure needs to report to the Director General/his or her delegate (not more than one level from the level of the DG).

12.2 The Chief Risk Officer (CRO) will coordinate risk management processes, monitor risk registers and table a report on the status of risk management in all Office of the Premier's meetings. (EMC and DMC) and Risk Management Committee meetings.

13. REVIEW

13.1 This strategy will be reviewed at least annually to ensure its continued application and relevance. Every employee has a part in this important endeavor and Premier and Management is looking forward to working with all staff members in achieving these aims.

14. RISK MANAGEMENT IMPLEMENTATION PLAN

The detailed Risk Implementation Plan below gives effect to the implementation of Risk Management Policy and this Strategy and set out all risk management activities planned for the 2021/2022 financial year.

14.1 OBJECTIVE

- The objective of the Risk Management Implementation plan is to facilitate the execution of risk management in the Office of The Premier for the financial year 2023/2024.

14.2 APPROACH

The risk management implementation plan shall take into consideration:

- The Risk Management Policy; and
- The Risk Management Strategy.

14.3 DETAILED RISK MANAGEMENT IMPLEMENTATION PLAN

CONFIDENTIAL

KPA	ACTIVITY(S)	OUTCOMES	DUE DATE	RESPONSIBLE PERSON	PROGRESS
Risk registers	Conduct Office strategic, operational and fraud risk annual assessment.	Approved Strategic, Operational, Fraud risk & Information Technology registers	4 th quarter of the 2025/2026 financial year	CRO	
	Conduct awareness campaign / survey consistent with the approved schedule	Improved risk management culture and understanding/knowledge across the Office.	2 campaigns per year 2 ND Quarter, and 3 rd Quarter 2025/2026 financial year	CRO	
Quarterly risk management activities report	Risk treatment plans implementation monitoring and identification of emerging risks	Consolidated risk management activities report produced	Quarterly 2025/2026 financial year	CRO	

CONFIDENTIAL

KPA	ACTIVITY(S)	OUTCOMES	DUE DATE	RESPONSIBLE PERSON	PROGRESS
Risk Management Committee meetings	Coordinate risk management committee meetings	Quarterly Risk Management Committee meetings minutes approved	Quarterly 2025/2026 financial year	CRO/RMC Secretariat	
Stakeholders engagements meetings	Coordinate engagement meetings with oversight structures/identified stakeholders per RM strategy	Consolidated risk management activities report produced	Quarterly 2025/2026 Financial year	CRO	
Risk Management implementation plan	Prepare a detailed Risk Management implementation plan for OOP incorporated to the risk management strategy	An approved risk management implementation plan for 2025/2026 financial year	4 th quarter of the 2025/2026 financial year	CRO	

KPA	ACTIVITY(S)	OUTCOMES	DUE DATE	RESPONSIBLE PERSON	PROGRESS
Review of Risk Management Literature	Circulating to staff members, incorporate reviews from for PRMU and recommendations by RMC members and lastly approved by Accounting Officer	Approved Risk management committee charter, Risk management policy, Risk management strategy and implementation plan and Risk champions charter	4 th quarter of the 2025/2026 financial year	Chief Risk Officer	

Recommended by:

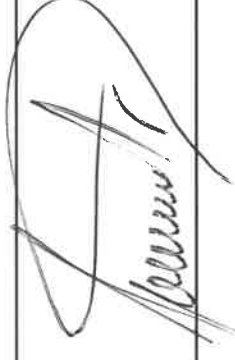


Mr. O.L Mokaila

Risk Management Committee Chairperson

Date: 27/03/2025

Approved / approved with comments/not approved:



M.P. Mogotlhe

Director General

Date: 31/03/2025