RISK MANAGEMENT STRATEGY 2025/2026

public works & roads

Department:
Public Works and Roads
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

CONTENTS

1. INTRODUCTION AND BACKGROUND

1.1 **Managing risks is a fundamental aspect of any organisation's operations**. The Public Finance Management Act (PFMA), through Section 38(1)(a)(i), requires the Accounting Officer to ensure that the Department maintains effective, efficient, and transparent systems of financial management, risk management, and internal control.

1.2 **The King IV Report on Corporate Governance** prescribes that an organisation should establish a risk management structure that will adequately identify measure, monitor, and control the risks involved in its various operations and lines of business.

1.3 **The Department of Public Works and Roads** has adopted an enterprise-wide risk management (ERM) strategy, which ensures that all key risks across the Department are addressed through a structured and systematic risk management process. This approach is designed to embed risk management into the Department's systems and processes, ensuring that our responses to risk remain relevant, proactive, and adaptable.

1.4 **All risk management efforts are aligned with the Department's strategic outcomes**. These efforts aim to ensure compliance with applicable legislation and meet the expectations of employees, communities, and other stakeholders in terms of good corporate governance.

1.5 **The risk management strategy serves as a framework for implementing the Department's risk management policy**. It outlines the steps needed to achieve the high-level objectives set forth in the risk management policy and provides a roadmap for improving the risk management process over time. Ultimately, the strategy will guide the Department towards achieving its desired level of risk maturity.

2. DEFINITIONS

2.1 **RISK** - An unwanted outcome, actual or potential, to the department'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 involves the potential for both negative and positive outcomes, and these outcomes are influenced by uncertainty, which can impact the achievement of an organization's objectives.

2.2 **RISK MANAGEMENT** - Risk Management is a continuous and proactive process, effected by management and other personnel, applied in strategic planning and across the department, designed to identify potential events that may affect the Department and manage risks to be within its risk tolerance and lastly to provide reasonable assurance that the Department's objectives will be achieved.

Risk Management It involves identifying, assessing, and managing risks to minimize their negative impacts and to take advantage of opportunities. The goal of risk management is to ensure that risks are appropriately understood and handled in a structured and systematic way, aligning with the organization's objectives.

2.3 ENTERPRISE-WIDE RISK MANAGEMENT (ERM) – A strategic process to enable the Department to identify, measure, and manage the entire range of business risks and opportunities it is facing.

2.4 RISK REGISTER – a tool used to record departmental risks.

2.5 RESIDUAL RISK –The remaining exposure after the mitigating effects of deliberate management intervention(s) to control such exposure (the remaining risk after Management has put in place measures to control the inherent risk).

2.6 INHERENT RISK - The exposure arising from risk factors in the absence of deliberate management intervention(s) to exercise control over such factors.

2.7 RISK APPETITE - a set maximum level of residual risk the department is willing to accept.

2.8 RISK ACCEPTABLE LEVEL - It is equal to or below the risk appetite. The department is not going to allocate resources to deal with this risk.

2.9 CORPORATE GOVERNANCE - Corporate governance involves mechanisms by which an organisation is directed and controlled. It is a corporate tool through which corporate management is held accountable for corporate conduct and performance. It is a strategic response to risk management.

2.10 INTERNAL CONTROLS - Mechanisms put into place to mitigate unacceptable levels of risk. Internal controls are a management's responsibility.

3. LEGAL MANDATE

A. The **Public Finance Management Act, 1999 (PFMA)**, supplemented by the relevant **Treasury Regulations**, legislates key governance best practices in public sector financial management. Section 38(1)(a) of the PFMA stipulates the following requirement:

"The accounting officer must ensure that the institution has and maintains effective, efficient, and transparent systems of financial and risk management, as well as internal control."

B. **Responsibility for Risk Management**:
The extension of risk management responsibilities, as outlined in Sections 45 and 57 of the PFMA, applies to all managers within the public sector. This implies that responsibility for risk management

extends throughout all levels of management, not just the accounting officer and internal audit. Every manager is accountable for managing risks within their scope of responsibility.

C. **Roles and Responsibilities for Risk Management**:

The **Treasury Regulations**, published in terms of the PFMA, define the roles and responsibilities for the implementation of the Risk Management strategy. Specifically, Sections 3.2 and 27.2.1 of the regulations address the following key aspects of risk management:

- **Regular Risk Assessments**:
  The accounting officer is required to ensure that regular risk assessments are conducted to identify emerging risks within the institution. These assessments must be comprehensive and consider both existing and potential risks.
- **Risk Management Strategy and Fraud Prevention Plan**:
  The institution's Risk Management strategy, which must include a fraud prevention plan, should guide the efforts of internal audit. The strategy helps prioritize internal audit activities and identifies the skills required by managers and staff to improve controls and effectively manage identified risks.
- **Communication and Embedding Risk Management**:
  The Risk Management strategy must be communicated to all officials within the institution. This ensures that risk management is integrated into the institution's language, culture, and day-to-day operations. It should become embedded in the behavior and mindset of employees at all levels.

4. APPLICABILITY OF THE STRATEGY

The **Risk Management Strategy** is designed to guide and inform the Department's approach to managing risks across all its operations. The principles and practices outlined in this strategy must be embraced by all levels of the department and by external parties that play a role in the Department's activities.

5. PURPOSE

5.1 Overview of the Risk Management Strategy

The Risk Management Strategy serves as a guiding framework for the Department to implement its Risk Management Policy. It provides a structured approach to integrate effective risk management practices across all departmental activities. The strategy ensures that these practices are clearly understood and can be applied consistently by all employees and relevant stakeholders. By fostering a unified approach, the department will be able to manage risks proactively and systematically, ensuring alignment with overall departmental goals and objectives.

5.2. Prevention and Mitigation of Risks

The **Risk Management Strategy** plays a crucial role in helping the Department to **prevent and minimize** the adverse effects of risks inherent in its operations. It establishes a proactive framework that allows the department to identify, assess, and address risks before they materialize into significant issues. The strategy underscores the importance of integrating risk management into all stages of **activities**, **functions**, or **projects**, emphasizing that risk management is an ongoing process throughout the lifecycle of every initiative.

Key aspects include:

- Applying risk management **throughout every project or function**, from initiation to completion, ensuring risks are continuously monitored and mitigated.
- Ensuring that **preventative measures** are taken before risks escalate into threats, safeguarding the department's objectives and outcomes.

This approach ensures that risk management is not just a reactive measure but an **integral part of the Department's operations** and decision-making processes.

6. OBJECTIVES

The department's risk management policy was reviewed for the 2025/26 financial year. In terms of this strategy, the department has established the following risk management objectives for the current strategy:

6.1 Create an environment for compliance with key statutory and best practice risk management requirements and principles, ensuring alignment with relevant regulations and standards;

6.2 Recognise risk management as critical to the achievement of the department's service delivery goals integrating risk considerations into decision-making and operational processes;

6.3 Ensure the identification, assessment, and management of material risks, both current and future, ensuring these risks are quantified, appropriately mitigated, and effectively managed across all levels of the Department;

6.4 Encourage a culture of zero tolerance for unethical conduct, fraud, and corruption, ensuring these issues are actively prevented and addressed in line with the Department's values and standards;

6.5 Develop a mature risk management culture where every line manager and employee understands their role in managing risks within their areas of responsibility. Employees will be encouraged to escalate risks that fall outside their authority or available resources to the appropriate level of management.

The Risk Management Strategy and its Implementation Plan will guide the Department in achieving these objectives, ensuring that risk management becomes an integral part of the Department's operations and decision-making processes.

7. DESIRED OUTCOMES

When effectively implemented and maintained, risk management will enable the Department to achieve the following outcomes:

- Sustainable and reliable delivery of services;
- Informed and reliable decision-making and planning which are underpinned by appropriate rigour and analysis;
- Improved governance, leading to increased stakeholder confidence and trust;
- Improved project management outcomes;
- Effective allocation and efficient use of resources;
- Reduced Wastage,losses and poor value for money;
- Prevention of Fraud and Corruption; and
- Improved Health and Safe Working Environment.

Risk management is recognized as an essential component of responsible management. As such, the Department adopts a comprehensive and structured approach to the management of risk. The features of this process are outlined in the Departmental Risk Management Strategy. It is expected that all programs, operations, and processes within the Department will be governed by this strategy. The intention is for these programs to work together in a consistent and integrated manner, with the overarching goal of minimizing risk as much as reasonably possible.

8. RISK MANAGEMENT MATURITY

A critical goal of the Risk Management Strategy is to elevate the Department's risk maturity level during the 2025/26 financial year and beyond. This means evolving the risk management culture and practices from a reactive stance to a more mature, proactive, and strategic approach.

As part of this improvement journey, the feedback from Provincial Risk Management will be utilized to enhance the Department's risk maturity. Provincial Risk Management has been reviewing and providing insights on the Department's current risk maturity, which will help in identifying gaps and areas for improvement. Furthermore, they are currently reviewing the risk maturity tool, which will serve as a key instrument in assessing and advancing the Department's overall risk maturity.

The planned actions outlined in the strategy will include:

- Strengthening the Department's existing risk management practices through regular assessments, feedback loops, and the implementation of lessons learned.
- Fostering continuous improvement in risk management capabilities, ensuring that staff are well-equipped to identify, evaluate, and manage risks effectively.
- Developing a more robust framework for handling risks, enhancing the Department's resilience and preparedness for both known and emerging risks.

By aligning these actions with organizational goals and leveraging insights from the Provincial Risk Management team, the Department aims to create an environment where risk management is ingrained in everyday decision-making and is continually evolving to meet new challenges.

9. RISK MANAGEMENT METHODOLOGY

The Department has adopted a comprehensive risk management approach aligned with industry best practices and international standards. This approach is based on guidance from key frameworks, including the Public Sector Risk Management Framework, ISO 31000: 2018 (Risk Management – Guidelines), and the COSO Enterprise Risk Management – Integrating with Strategy and Performance 2017.

The department aims to implement a structured, organization-wide risk management process that will:

FOCUS AREA	DESCRIPTION
Governance and Culture	This stage assists with setting the tone from the Top in the department, establishing responsibilities, and embedding the anticipated culture. i.e. establishment of a Risk Committee, Embedding of risk culture, establishment of Risk Management roles, and the capacitation thereof.
Strategy & Objective Setting	This stage provides the context of how the Department operates and its environment. It is in this phase, that the Risk Management process is aligned to the Departmental strategy. i.e. defining risk appetite, integration of the strategic risk process, and the Strategic planning process
Establishing the context, scope, and criteria	At this stage, both external and internal factors are considered when identifying and managing risks associated with the achievement of strategic and operational objectives.
Risk Identification	This stage requires the identification of risk sources, areas of impact, events, causes, and possible consequences to form a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate, or delay the achievement of objectives
Risk Analysis	this sub-process considers the range of risk root causes, sources of risk, risk impacts/consequences, and likelihood/probability of risk occurrence to produce risk ratings.
Risk Evaluation	Risks must be quantified and prioritized through a systematic risk assessment process.
Risk Treatment	Appropriate response strategies must be developed and evaluated to reduce or eliminate threats and events that create risks. In addition, selecting one or more options for reducing risks including funding and other resource considerations.
Review & Revision	The entire risk management system must be periodically reviewed and evaluated to ensure continual improvements. Continual monitoring and reviewing of risk profiles is essential to maintain the effectiveness and appropriateness of the risk management profiles, including more specifically, risk treatment plans, and risk assessments and to identify emerging risks.
Information Communication and Reporting	The product of the risk assessment process is recorded in the form of risk registers which will ultimately be used for reporting. Appropriate communication and consultation processes must be used to communicate relevant risk information to officials and stakeholders to equip them to identify, assess, and respond to risks.

10. RISK MANAGEMENT STRUCTURE

The diagram below (Figure 1) provides the risk management structure, and thus an indication of people and formations that must be assigned risk management roles and responsibilities at a departmental level:

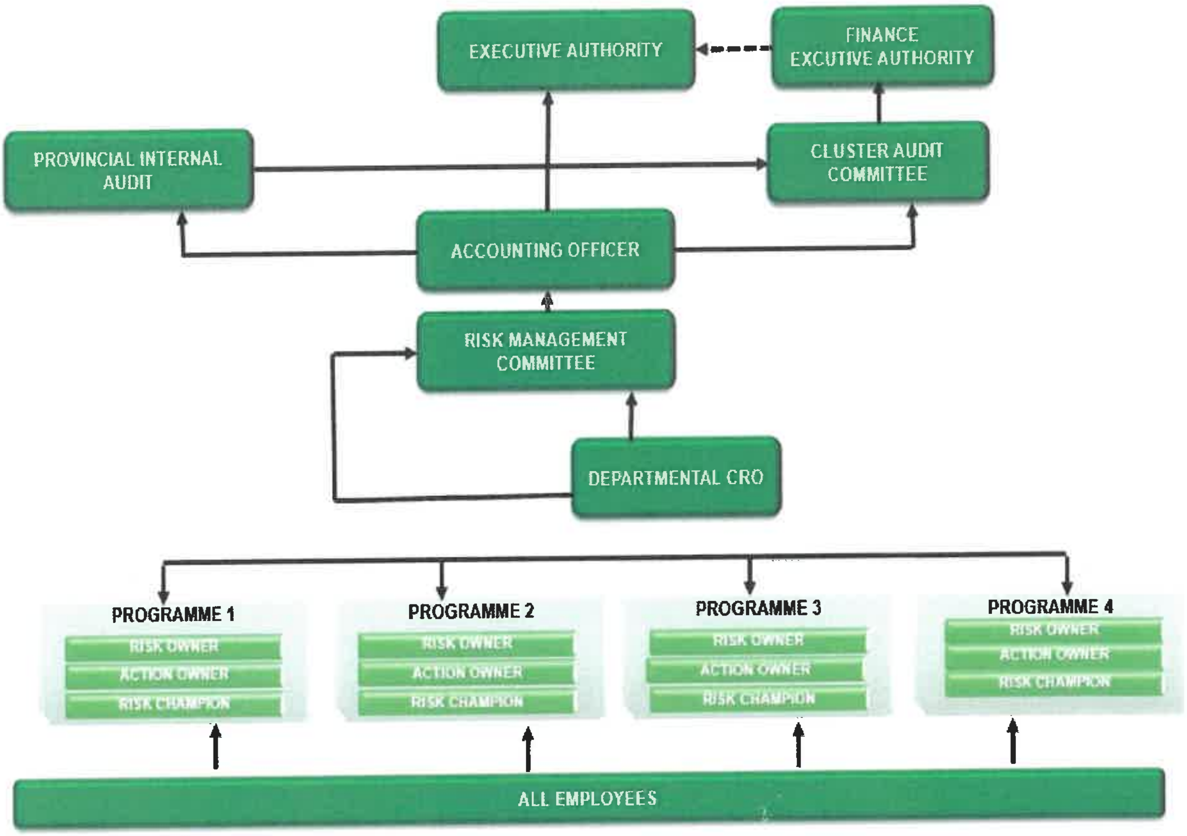

FIGURE 1: RISK MANAGEMENT STRUCTURE

- The Risk management function reports to the Head of the Department and the Executive Authority to ensure its integration and effectiveness within the Department.
- The Chief Risk Officer (CRO) will coordinate risk management processes, monitor risk registers, and present reports on the status of risk management at all Departmental Committee Meetings (EMC & DMC), Risk Management Committee Meetings (RMC), and Provincial Risk Management Forum.

11. RISK APPETITE STATEMENT

The Department recognizes that the pursuit of its objectives and service delivery commitments inherently involves taking risks. However, it is essential to balance the need for risk-taking with the potential negative consequences. The key question is not whether to take risks but how much risk is acceptable in the pursuit of its goals and which risks need to be actively managed to avoid adverse outcomes. This distinction ensures that risk management becomes an integral part of the Department's culture rather than an isolated activity.

In line with this approach, every line manager and employee are considered a risk manager within their area of responsibility. They are tasked with identifying, managing, and escalating risks as necessary. In instances where risks exceed the scope of an individual's authority or resources, it is their responsibility to escalate the issue to the appropriate level of management for resolution.

The Department's *Risk Appetite* is clearly defined to articulate the level and types of risk it is willing to accept. This is outlined in terms of the residual risk rating (Risk Rating 5-9 and below), which is subject to ongoing monitoring and periodic reviews to ensure that these risks remain within acceptable levels.

The Department evaluates its risks by analysing both inherent and residual risks, using a systematic approach based on the Public Sector Risk Management Framework, the Department's Risk Management Policy, and other relevant documents. The following risk categories and corresponding appetite levels have been established:

RISK RATING	RISK MAGNITUDE	RISK APPETITE STATEMENT	
		RISK APPETITE CATEGORY	DESCRIPTOR
20 - 25	**Maximum**	**Averse**	These risks ***cannot be tolerated*** at their current levels. Immediate action must be taken to cease activities that pose these risks until appropriate controls are developed and implemented to reduce them.
15 - 19	**High**	**Cautious**	These risks are deemed ***unacceptable*** unless unique conditions apply. Major interventions are required to bring them to an acceptable level. The benefits of control interventions must outweigh the costs.
10 - 14	**Medium**	**Cautious**	These risks ***must be mitigated***, provided the benefits of risk reduction exceed the costs of implementing controls.
5 – 9	**Minimum**	**Minimalist**	Risks in this category are ***mostly acceptable*** and will be continuously monitored and periodically reviewed to ensure they remain within an acceptable threshold.
1 – 4	**Low**	**Minimalist**	Risks at this level ***are accepted*** at their current levels, no treatment is required.

The Department is committed to dedicating resources to manage and control its risk exposures to an acceptable level. However, it is also acknowledged that it is not always possible to mitigate all risks to the desired level. In these cases, the Department applies a cost-benefit analysis to determine the most efficient and effective risk management strategy. This approach ensures that the Department allocates its resources efficiently while addressing the most critical risks.

12. RISK PROFILES

Departmental risk registers will be compiled in a broad-based manner to cover all major types of risks, including strategic, financial management and reporting/financial statements, IT, Fraud, OHS, compliance risks, and business unit risks beyond the control of management. Risk registers are regarded as dynamic documents that must be reviewed and/or updated at least quarterly or as circumstances dictate (not limited to media reports, incidents, business/activities change, fourth industrial revolution/technology, etc.).

The following risk categories must be included in the Department's risk profiles:

12.1 Strategic Risks:

These risks arise from the Department's strategic decisions, which are based on the objectives and outcomes outlined in the Department's Strategic Plan. Strategic risks could involve external factors such as changes in legislation, government policies, or shifts in public opinion that may affect the Department's ability to meet its goals. Effective identification and management of strategic risks are crucial for achieving long-term objectives and ensuring alignment with the Department's mission.

12.2 Operational Risks:

Operational risks encompass those that arise from the Department's day-to-day activities. These risks can stem from internal processes, systems, employees, contractors, and external events such as economic conditions or natural disasters. Specific operational risks include threats such as fraud, ethical breaches, ICT vulnerabilities, and the potential disruptions caused by emergencies (e.g., pandemics). Identifying these risks early allows the Department to mitigate their impact on service delivery.

12.3 Project-Specific Risks:

These are risks associated with specific projects undertaken by the Department. Whether these projects involve policy changes, infrastructure development, or reconfigurations, it is essential to identify risks that could hinder their successful execution. This may include technical issues, budget overruns, changes in scope, or delays caused by external factors. By assessing and addressing these risks proactively, the Department can increase the likelihood of project success and minimize disruption to service delivery.

12.4 Emerging Risks:

The Department must remain vigilant in identifying emerging risks, such as those related to technological advancements (e.g., AI, cybersecurity) and global challenges (e.g., climate change, geopolitical instability). Recognizing these risks early allows for the development of forward-thinking mitigation strategies.

The risk registers should not be static; they must evolve as the Department encounters new risks and as existing risks change in magnitude or likelihood. Management should facilitate risk identification workshops regularly, engaging key stakeholders to review and assess risk levels and ensure that new interventions are identified where weaknesses in current risk management strategies are found. These interventions should aim to enhance operational efficiency, improve risk mitigation, and support the achievement of the Department's strategic objectives.

13. RISK ASSESSMENT

The department follows a structured and systematic approach to risk assessment, ensuring that each identified risk is thoroughly quantified and evaluated for its potential impact on departmental objectives. This process helps prioritize risks, allocate resources effectively, and implement mitigation strategies for the most critical issues. To ensure consistency and effectiveness, the department has adopted the following risk management approach and process for the upcoming 2026/27 financial year:

13.1 Risk Assessment Process

The department will conduct comprehensive risk assessments at both the departmental and business unit levels. The goal of these assessments is to identify potential risks, evaluate their impact, and develop effective mitigation strategies. The following steps outline the key phases of the risk assessment process:

(a) Identifying Risks and Root Causes

The first step involves identifying risks that apply to each business unit, as well as their underlying root causes. This process will include analysing both internal and external factors that could potentially threaten the department's ability to meet its objectives. These risks can range from operational challenges, regulatory changes, technology failures, to external threats such as natural disasters.

(b) Evaluating Likelihood and Impact

Once risks are identified, the likelihood of their occurrence and their potential impact on the department's objectives will be assessed. The department will determine the **inherent risk exposure** for each identified risk. This evaluation helps to understand the severity of each risk and the likelihood that it will materialize. By assessing both the **likelihood** (the probability of occurrence) and **impact** (the potential consequences), the department can prioritize risks based on their significance to the organization.

(c) Identifying Controls to Mitigate Risks

In this step, the department will review existing risk controls and determine the **ideal controls** needed to mitigate the identified risks. This involves developing strategies that will effectively reduce or eliminate the risks to an acceptable level. The department may consider various options such as process improvements, enhanced security measures, additional staff training, or technological interventions.

(d) Risk Rating (Pre-Control Level)

Following the identification of risks and controls, the risks will be rated according to their **inherent risk exposure**. This pre-control rating will consider both the **likelihood** and **impact** of the risk using an adopted risk matrix scale. The scale will help categorize risks into different levels, such as high, medium, or low, based on the severity of the potential consequences. This rating will also be applied to assess the **effectiveness** of existing controls in managing these risks. The effectiveness of controls will be reviewed to determine whether adjustments are necessary.

The risk assessment process incorporates a robust risk evaluation framework, including the **Likelihood Rating Scale**, **Impact Rating Scale**, **Control Effectiveness Rating Scale**, and **Risk Exposure Levels**. This ensures that risks are not only identified and evaluated but also that mitigation efforts are aligned with the potential severity of each risk.

The 2026/27 risk assessments will be conducted during the 2025/26 financial year. The following rating scales will be applied when conducting the risk assessments:

Likelihood Rating Scale:

This scale measures the probability of a risk occurring, helping to assess how often a risk may manifest within a certain timeframe.

Descriptor	Level	Definitions
Rare	1	The risk is conceivable but is only likely to occur in extreme circumstances.
Unlikely	2	The risk occurs infrequently, with a low probability, within the next three years.
Moderate	3	There is an above-average chance that the risk will occur at least once in the next three years.
Likely	4	The event is likely to occur at least once within the next 12 months.
Common	5	The event is likely to occur more than once within the next 12 months.

Impact Rating Scale:

This scale measures the severity of the consequences if a risk materializes, assisting in understanding how critical a risk is to the achievement of the department's objectives.

Descriptor	Level	Definitions
Insignificant	1	Negative outcomes or missed opportunities are likely to have a relatively negligible impact on the ability to meet its objectives.
Minor	2	Negative outcomes or missed opportunities are likely to have a relatively low impact on the ability to meet its objectives.
Moderate	3	Negative outcomes or missed opportunities are likely to have a relatively moderate impact on the ability to meet its objectives.
Major	4	Negative outcomes or missed opportunities that are that are of substantial importance on the ability to meet its objectives
Critical	5	Negative outcomes or missed opportunities that are of critical importance to the achievement of its objectives.

Control Effectiveness Rating Scale:

The effectiveness of current controls is evaluated to determine their adequacy in mitigating the risks identified during the assessment process. This helps determine whether the current controls are sufficient or need further improvement. The **Control Effectiveness Rating Scale** helps categorise control measures based on their performance.

Descriptor	Effectiveness Rating	Definition
Very Good	5	The controls in place are working at an optimum level
Good	4	The controls in place are addressing the risks but are not working at an optimum level

Descriptor	Effectiveness Rating	Definition
Satisfactory	3	The controls in place are working at an acceptable level, but more can be done to strengthen these controls
Weak	3	The controls in place need to be strengthened, or new controls need to be implemented
Unsatisfactory	1	The controls in place are ineffective, and new controls need to be implemented

Risk Exposure

Risk exposure is determined based on the combined assessment of likelihood and impact, guiding the appropriate response and prioritization of resources.

Risk rating	Risk magnitude	Response
20 - 25	**Maximum**	Unacceptable level of risk. Immediate action must be taken to mitigate the risk (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 - Low level of control intervention required if any
1 – 4	**Low**	Acceptable-No action required

13.2 Fraud Risk Rating

In addition to general risk management, the department has a dedicated framework to assess and mitigate fraud-related risks. Fraud risks will be evaluated separately but in conjunction with the overall risk assessment process to ensure that specific controls are in place to address potential fraudulent activities.

Likelihood Rating Scale:

This scale measures the probability of a risk occurring, helping to assess how often a fraud risk may manifest

Descriptor	Level	Definitions
Rare	1	Fraud is conceivable but is only likely to occur in extreme circumstances
Unlikely	2	Fraud may occur infrequently and is unlikely to occur

Descriptor	Level	Definitions
Moderate	3	There is an above-average chance that fraud will occur
Likely	4	Fraud could easily occur
Common	5	Fraud is already occurring

Impact Rating Scale:

This scale measures the severity of the consequences if the fraud risk materializes.

Descriptor	Level	Definitions
Insignificant	1	There is a 90-100% chance that the controls will prevent fraud. **(Unacceptable-Action must be taken)**
Minor	2	There is a 70-89% chance that the controls will prevent fraud. **(Unacceptable-Action must be taken)**
Moderate	3	There is a 50-69% chance that the controls will prevent fraud. **(Unacceptable-Action must be taken)**
Major	4	There is 30-49% chance that the controls will prevent fraud. **(Unacceptable-Action must be taken)**
Critical	5	There is 1-29% chance that the controls will prevent fraud. **(Unacceptable- Action must be taken)**

Fraud Risk Exposure

The department will categorize risks into different levels of exposure based on their likelihood and impact ratings. This categorization helps determine the urgency of actions needed for mitigating each risk.

Risk rating	Risk magnitude	Response
20 - 25	Maximum	Unacceptable- Action must be taken immediately – considering zero tolerance stance to fraud
15 - 19	High	Unacceptable- Action must be taken – considering zero tolerance stance to fraud (Major level of control intervention)
10 - 14	Medium	Unacceptable- Action must be taken – considering zero tolerance stance to fraud (Moderate level of control intervention)
5 – 9	Minimum	Unacceptable- Action must be taken – considering zero tolerance stance to fraud (Update routine control procedures)
1 – 4	Low	Unacceptable- Action must be taken – considering zero tolerance stance to fraud (Update routine control procedures)

14. RISK RESPONSE AND TREATMENT

Risk assessment participants are responsible for identifying both the current controls in place to mitigate inherent risks and developing treatment plans aimed at enhancing risk mitigation. Treatment plans will be specifically focused on areas where management identifies weaknesses, as well as opportunities where new interventions may improve process efficiencies. Treatment plans will then be assigned to respective risk owners for implementation and continuous monitoring.

Risk response and treatment refer to the process of formulating actions to reduce or mitigate the impact or likelihood of risks that have been deemed unacceptable during the risk evaluation process. Risk treatment involves identifying options to address each risk, evaluating those options, preparing treatment plans, and closely monitoring the execution of these plans. In some cases, a combination of risk treatment options may be necessary to effectively manage a risk.

The department will consider the following response strategies when addressing risks:

1. **Avoiding the Risk**: This strategy involves changing the approach or ceasing the activity that generates the risk. For example, if the risk is too high, the department may decide to stop the activity or alter the strategy to eliminate the risk.
2. **Treating the Risk**: This involves taking deliberate actions to reduce the risk to an acceptable level. Common treatments may include implementing stronger internal controls, process improvements, or additional safeguards to manage the risk effectively.
3. **Transferring the Risk**: In this case, the department may shift the risk to another party, often through outsourcing or entering into partnerships. For instance, contracting services to a third-party vendor, transferring insurance risks, or outsourcing certain business functions can help mitigate the department's exposure to specific risks.
4. **Accepting the Risk**: This approach is used when alternative strategies are not viable due to cost constraints or when the risk is considered within acceptable levels. Management may decide to take no immediate action but will continue to monitor the risk for any changes.
5. **Exploitation (for positive risks/opportunities):** This strategy focuses on capitalizing on opportunities that arise from positive risks (opportunities). Rather than avoiding or mitigating them, the organization takes actions to maximize the benefit or value derived from the risk.

The department's **risk appetite** — the level of risk deemed acceptable — will guide the selection of the appropriate risk management strategy for each identified risk. By aligning risk treatment strategies with the department's risk appetite, management can ensure that the department's resources are efficiently used, and risks are kept within tolerable boundaries.

15. REVIEW & REVISION

Ongoing monitoring and regular reviews of risk profiles, risk management practices, and related literature are essential to ensure the continued effectiveness and relevance of the risk management process. This will be achieved through the following actions:

- **Annual Review**: A comprehensive annual review and evaluation of the entire risk management system (including a Risk Maturity Assessment) will be conducted by assurance providers. This ensures that the risk management framework operates effectively and in line with best practices.
- **Quarterly Review**: The risk registers and the effectiveness of existing risk mitigation plans will be reviewed and evaluated on a quarterly basis. This allows for timely updates and adjustments in response to changes in the risk landscape.

- **Emerging Risks**: New or emerging risks will be identified and evaluated on an ongoing basis. These risks will be assessed during quarterly risk monitoring and evaluation to ensure that they are addressed promptly and appropriately.

Regular reviews ensure that the department's risk management approach remains dynamic, adaptable, and aligned with the evolving internal and external environment.

16. INFORMATION COMMUNICATION AND REPORTING

Effective and continuous communication is vital for successful monitoring and management of risks. Ensuring that relevant stakeholders receive timely and accurate reports about the current status of financial, operational, and risk-related data is crucial. These reports should be supported by adequate and appropriate systems that facilitate informed decision-making within the time frame that enables employees to carry out their responsibilities effectively.

The primary purpose of communication and documentation is to ensure that all employees are aware of the risks they face, the available mitigation strategies, and how to make informed decisions within the constraints of available resources. Effective communication fosters a culture of transparency and shared understanding, helping the organization proactively manage risks and adopt best practices.

To ensure robust communication and reporting, the department will take the following steps:

- **Formal Communication of Responsibilities**: Communicate risk management responsibilities to all relevant personnel. This includes ensuring that employees at all levels understand their role in managing risk and escalating issues when necessary.
- **Agreement on Risk Mitigation Plans**: Risk mitigation plans, including timelines for completion, should be discussed, agreed upon, and documented with the relevant risk owners. This ensures accountability and alignment across the organization.
- **Mechanisms for Reporting and Escalation**: In addition to risk workshops, provide employees with accessible avenues for reporting and escalating risks. This ensures that potential threats are identified and addressed on time, regardless of the reporting structure.
- **Quarterly Reporting to Management and Oversight Bodies**: Risks and the status of risk mitigation efforts will be reported regularly (quarterly) to senior management and oversight structures, such as the Audit Committee and the Risk Management Committee. This provides transparency and facilitates informed decision-making at the highest levels.
- **Annual Reporting on Risk Management Effectiveness**: The effectiveness of the department's risk management practices will be reported in the annual report. This includes detailing how strategic risks have been managed and mitigated, along with an assessment of the overall success of risk management initiatives.

By ensuring that risk management information is communicated effectively throughout the organization, the department will foster a culture of proactive risk management, transparency, and continuous improvement.

17. PERIOD OF REVIEW AND AMENDMENT

This Risk Management Strategy will be reviewed on an annual basis to ensure its continued relevance and effectiveness in addressing emerging risks and organizational changes. If amendments are required due to shifts in the organizational landscape, regulatory updates, or any other factors, such amendments will be made promptly and incorporated into the strategy.

Any revisions will be communicated to all relevant stakeholders, and updated versions will be distributed to ensure alignment and consistency in the execution of risk management practices across the department.

18. RECOMMENDATION AND APPROVAL

The Risk Management Strategy is hereby recommended for approval by the Risk Management Committee and shall be formally approved by the Head of Department.

Recommended by the Risk Management Committee:

Signature: ____________________

Date: 19 March 2025

Approved by the Head of Department:

Signature: ____________________

Date: 18/03/25

ANNEXURE A: RISK MANAGEMENT IMPLEMENTATION PLAN 2025/26

Planned Action	Detailed Actions	Outputs	Due date and responsible person
Review the risk management policy for 2025/26	CRO to review and update the policy and submit it to the Risk Management Committee (RMC) to recommend to the Accounting Officer for approval.	Approved risk management policy	Chief Risk Officer 31 March 2025
Review the risk management strategy and plan for 2025/26	CRO to review and update the strategy and submit it to the Risk Management Committee (RMC) to recommend to the Accounting Officer for approval.	Approved risk management strategy	Chief Risk Officer 31 March 2025
Risk Management Integration with Strategic Planning	Ensure that risk management is a key part of the strategic planning process. • Conduct strategic risk assessments as part of the strategic planning cycle. • Include risk-based decision-making when developing or updating strategic goals. • Ensure that all departmental outcomes have an associated risk treatment plan	Strategic plans that reflect the department's risk management approach/vision etc.	Senior Management and Risk Management Unit
Development of a Strategic Risk Register	Develop a comprehensive risk register specifically for strategic risks, alongside operational and project-specific registers.	Strategic risk register	Chief Risk Officer 31 March 2025
Embedding of Risk Management	Foster a risk-aware culture within the Department. • Include risk management principles and practices in onboarding for new employees. • Promote the idea that risk management is everyone's responsibility and part of the organizational culture.	A risk-aware workforce and integrated risk management practices.	Chief Risk Officer Bi-Annually
Raising awareness and risk management training	Launch internal campaigns to raise awareness and educate employees about risk management practices.	Increased employee awareness of risk management.	Chief Risk Officer Ongoing

Planned Action	Detailed Actions	Outputs	Due date and responsible person
	• Organize risk management awareness weeks, events, or campaigns. • Distribute risk-related materials (flyers, newsletters, etc.) that highlight the importance of risk management. • Share case studies of successful risk mitigation or lessons learned from incidents within the department.		
Risk Management Committee Charter	Review existing RMC Charter Appoint members to the Risk Management Committee	Approved risk management committee charter Appointment letters	Chief Risk Officer 30 June 2025
Facilitate enterprise-wide risk assessments	Facilitate risk identification and assessment sessions. Analyse information and develop risk assessment reports.	Draft strategic, operational, fraud, and ICT risk registers.	Chief Risk Officer Quarter 3&4
Quarterly Risk Monitoring and Identification of emerging risks	Review the status of the implementation of treatment plans Collect and validate portfolio of evidence for implemented plans. Re-evaluate the impact of treatment plans on the risks. Discuss emerging risks with employees and risk owners and report to the risk management committee.	Quarterly risk Management report Updated risk registers	Chief Risk Officer All Managers Quarterly

Planned Action	Detailed Actions	Outputs	Due date and responsible person
Convene risk management committee meetings	Convene Risk Management Committee meeting. Submit the RMC report to the audit committee.	Minutes of RMC meetings RMC Report	Chief Risk Officer, RMC Quarterly
Monitor and plan actions for reports of assurance providers	Compile audit action plans for Internal Audit and AGSA audit reports Compile action list for reports of Provincial Risk Management	Audit action plans Quarterly Risk Management Report	Chief Risk Officer Ongoing
Continuous Improvement Based on Committee Feedback	Collect feedback from RMC members on the current risk management process, meeting effectiveness, and any changes required.	RMC Self-Evaluation template	RMC Members and Risk Management Unit.