EASTERN CAPE DEPARTMENT OF SOCIAL DEVELOPMENT

RISK MANAGEMENT STRATEGY
2025-2028

TABLE OF CONTENTS

ABBREVIATIONS

Abbreviation	Description
ECDSD	Eastern Cape Department of Social Development
PFMA	Public Finance Management Act
NT	National Treasury
COSO	Committee of Sponsoring Organizations of Treadway
HOD	Head of Department
AC	Audit Committee
CRO	Chief Risk Officer
CAE	Chief Audit Executive
AG	Auditor General
FPP	Fraud Prevention Plan
IA	Internal Audit

1. DEFINITIONS OF TERMS

No.	Terms	Definition
1.	**Accounting Officer**	The Head of department as defined in the Public Service Act.
2	**Assurance Function**	These are functions rendered by Internal & External Audit.
3.	**Audit Committee**	An independent committee constituted to review the control, governance, and risk management within the Department, established in terms of section 77 of the Public Finance Management Act.
4.	**Risk Cause**	Underlying factors/ causes/ weakness that would give rise to a risk(s).
5.	**Chief Risk Officer**	A senior official who is the head of the risk management unit.
6.	**Risk Consequence**	The consequence is the impact of risk on the department if the risk materializes.
7.	**COBIT 5**	Refers to Control Objectives for Information and related Technology (COBIT). COBIT 5 is a Governance and Management framework for ICT. COBIT 5 has been adopted by the DPSA through the promulgation of the Corporate Governance of ICT Policy Framework.
8.	**CONTROL**	The means used to manage a risk. A policy, procedure, device, system, communication, or other action that acts to reduce likelihood and impact of risk in departmental objectives and/or to ensure compliance with the law.
9.	**CRISC**	Refer to Certified in Risk and Information Systems Control. CRISC is a sponsored certification by ISACA who is in turn, endorsed by DPSA through Corporate Governance of ICT Policy Framework.
10.	**Department**	Refers to the Eastern Cape Department of Social Development
11.	**Executive Authority**	The Member of the Executive Council of a department who is accountable to Provincial Legislature for that department.
12.	**Impact**	This is the potential magnitude of the impact on the department's objective, should the risk occur. This must be assessed on the basis that management has no specific controls in place of addressing the risk, i.e., without any controls in place, what will the impact of this risk be on the department?
12	**Inherent Risk**	The exposure arising from risk factors in the absence of deliberate management intervention(s) or internal control. It is considered a raw risk.

14	**Likelihood**	This is the chance that the identified risk will occur on the basis that there are no specific controls in place to address the risk.
15	**Operational Risk**	Risk of loss due to deficiencies of failure in operational processes, people, information systems, management failures and external events including legal risks.
16	**Other Official**	An official other than the Accounting Officer/MEC, SMS members, CRO, and his/her staff.
17	**Residual Risk**	The remaining exposure after the mitigating effects of deliberate management interventions(s) to control such exposure (the remaining risk after Management has put in place measures to control the inherent risk).
18	**Risk**	An unwanted outcome, actual or potential, to the department's service delivery and other performance objectives, caused by the present risk factor(s). Some risks also present upside potential, which Management must be aware of and be prepared to exploit. This definition of risk "risk" also encompasses such opportunities.
19	**Risk Appetite**	The amount of risk that the Institution is willing to accept. Risk Appetite is set at a strategic level or at a risk category level.
20	**Risk Profile**	Is the register of all risk identified at a particular point in time, which indicates risk description, risk rating, risk managers and risk mitigation strategies.
21	**Risk Management**	A systematic and formalized process to identify, assess, manage, and monitor risks.
22	**Risk and Anti-Corruption Management Committee**	A committee appointed by the Accounting Officer/Authority to review the Institution's system of risk management.
23	**Risk Tolerance**	The amount of risk the Institution is capable of bearing (as opposed to the amount of risk it is willing to bear).
24	**Strategic Risk**	the potential for a department's strategic decisions or external events to undermine its ability to achieve its goals and long-term objectives, potentially impacting in its viability and stakeholder value.

2. BACKGROUND

Eastern Cape Department of Social Development (ECDSD) is required to comply with the Public Finance Management Act No. 1 of 1999 as amended, National Treasury Regulations as amended, Public Sector Risk Management Framework, relevant circulars, while adherence to the King IV Report on Corporate Governance

Managing risks is fundamental to the vision and mission of the department. The PFMA through section 38(a)(i) requires the Accounting Officer to ensure that the Department has and maintains effective and transparent systems of financial and risk management and internal control.

King IV recommends that the governing body (risk structure) should govern risk in a way that supports the organization in setting and achieving its strategic objectives.

The ECDSD will adopt an enterprise-wide risk management strategy which means that every risk in each part of the Department will be included in a structured and systematic processes and will become embedded into the Departments systems and processes, ensuring that responses to risk remain current and dynamic. All risk management efforts will be focused on supporting the Departments objectives. Equally, they must ensure compliance with relevant legislation, and fulfil the expectations of employees, communities, and other stakeholders in terms of corporate governance.

The department has therefore developed the following policies to emphasize its stance towards the effective management of risks in the department:

Risk Management Policy

Fraud Prevention and Investigation Policy

Whistle Blowing Policy

Integrity Management Policy

Loss Control Policy

The development of the risk management strategy has considered the above-mentioned policies and the Department's risk profile. A Fraud Prevention Plan and Risk Management Implementation Plan have been developed as part of the Strategy.

The Accounting Officer of the Department is spearheading this strategy and accordingly puts in place a Risk and Anti-Corruption Management Committee to drive it.

3. PURPOSE

The purpose of this strategy is to ensure effective implementation of the risk management and fraud prevention policy. It is developed to:

- To set a plan of action to improve the Department's risk management maturity.
- Discourage inefficiencies and combating fraud and corruption.
- Provide for the management of risk within the Department with the intention of enhancing service delivery, ensuring improved efficiency, and promoting excellence.
- Ensure that the Department is in line with the best practice with regards to improving governance and accountability.
- Entrench a risk management culture in the processes and systems of the Department across all spheres and levels.
- Ensure an integrated approach in the management of risk in the department by adopting a common language, process, and methodology.
- Foster a culture of good governance and ethical conduct in the Department.

4. SCOPE OF APPLICABILITY

This strategy is applicable to all employees of the Department and will be effective from the date of approval by the Accounting Officer.

5. RISK MANAGEMENT MATURITY

The department will adopt the National Treasury's Risk Management Maturity ("RM Maturity" to measure its level of maturity with regards to risk management. This will assist the department in developing mechanisms to improve its maturity. Further to National Treasury Risk Management Maturity tool, the Department will utilise Internal Audit reports on Risk Management to improve risk management processes. The RM Maturity is made up of five (5) levels, summarized as follows:

I. **Level 1 – Initial:** A risk management framework is not in place. Risk Management practices are ad-hoc and unsystematic.

II. **Level 2 – Fragmented:** An approved risk management framework (incorporating policy and implementation strategy) is in place and has been communicated throughout the department, however implementation at a low level at this stage.

III. **Level 3 – Top Down:** Departmental-wide risk assessments have been completed and the necessary departmental capacity and structure to support risk management are in place. Risk management processes, practices and systems satisfy all legislative requirements at this stage but have limited influence on the control of the environment.

IV. **Level 4 – Systematic:** Risk Management is firmly embedded in the department. Metrics to measure the value-added to risk management are in place. Aggregated risk management information is circulated to relevant officials and oversight structures as a matter of routine. Risk Tolerance parameters have been established for all major categories of risk. Management of risk is subjected to close prudent risk taking. Risk Management has a significant influence on the control environment at this stage.

V. **Level 5 – Risk Intelligent:** The institution has reached a state where the risks taken are consistent with its risk tolerance. Risk embedded in strategy setting, planning, and capital allocation**.** The focus of the institution has shifted firmly to employing risk management to optimise effectiveness, efficiency, and economy within its operations. Early warning risk indicators, risk modelling scenarios, and industry benchmarking initiatives are used as risk intelligence capabilities. Using such will ensure that risks of performance measurement and incentives are achieved.

The department has developed a Risk Management Implementation Plan to ensure that the department matures to the next level by the end of the Financial Year. The Risk Management Implementation Plan document will be reviewed annually to ensure that the department has a consistent risk management improvement strategy in terms of its risk management maturity, and maintenance of the highest level of risk management maturity in the department.

6. THE RISK MANAGEMENT METHODOLOGY

The Department adopts the principles of COSO framework and ISO 31000 as additional guidance on implementation of enterprise-wide risk management in the department.

6.1. Adopted process outlined below:

6.1.1 Objective ⇒ Risk ⇒ Control

It will start with reviewing the strategic objectives of the department and identifying risks (threats and opportunities) that could impact those strategic objectives and assess them in terms of likelihood and impact considering risk appetite limits of the department.
= **strategic planning and risk identification**

6.1.2 Events with negative impact to be listed, classified and analyzed = **risk assessment**

6.1.3 Controls to be listed classified and analyzed = **control self-assessment**

The Departmental objectives will be viewed in the context of four categories as per the COSO framework.

- Strategic
- Operations
- Reporting
- Compliance

6.2. The Department shall ensure functionality of the appointed risk management committee.

6.3. The CRO will coordinate the risk management processes in the Department.

6.4. The Department shall set the risk appetite/tolerance or acceptable levels to facilitate decision making concerning how to address the risks.

6.5. The CRO shall conduct risk education awareness to the other officials of the department during the financial year.

6.6. The Department shall Formalise accountability through inclusion of risk management responsibility to other relevant officials' performance agreements.

6.7. The Department will develop an action plan against the risk maturity level and monitor this plan ongoing and report to the Risk and Anti-Corruption Committee.

6.8. Conduct annual risk assessments prior to the beginning of a financial year (31 March yearly) and this process entails:

- Identification of risk linked to departmental outcomes.
- Assessment and evaluation of the identified risks
- Adopting appropriate risk responses to manage the risks.
- Timeous implementation of risk responses by management.

6.9. The above process will produce a risk register for the Department.

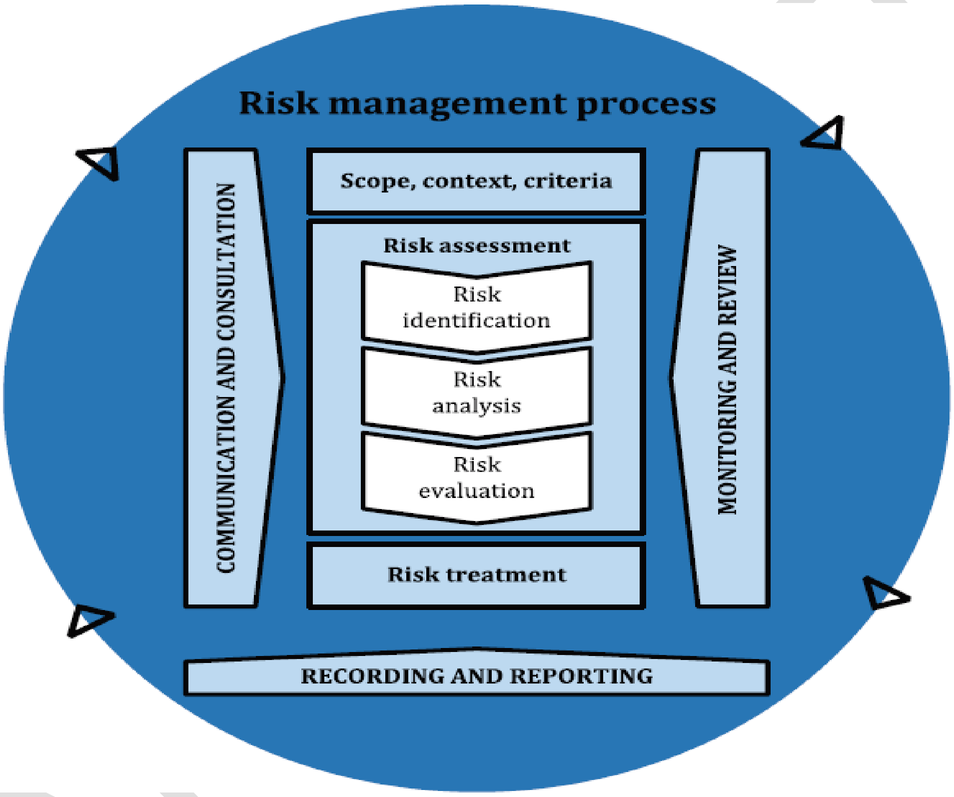
6.10. **Fraud prevention plan**: Detailing initiative-taking measures that must be implemented timeously, to manage institutional fraud risks.

6.11. **Ethics Management Plan**: Effective analysis of ethics risks ensuring consistency in approach between the ethics and corruption risk assessment and other risk assessment initiatives at the department.

6.12. **Monitoring activities**: This detail measures to monitor risk management processes and fraud prevention plan on a pre-set basis.

7. RISK MANAGEMENT PROCESS

The Department has adopted a risk management process which is in line with ISO 31000. The prescribed process that must be followed when conducting risk assessments is shown in the diagram below and outlined in detail further in the sections of this document:



8. ESTABLISHING SCOPE, CONTEXT 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. Techniques such as brainstorming, Delphi technique, surveys, review of data reports, structured and semi-structured interviews are used to arrive at appropriate conclusions.

9. RISK ASSESSMENT

9.1 Risk Identification

It is an integral part of risk management and management's responsibility. It cannot be relegated to a one-time static process. The department is operating in a dynamic environment with constant political changes. It is therefore prudent for management to consider risk identification as ongoing and continuous.

One must ask him/herself the following question: **What are the threats relative to the achievement of a specific objective?**

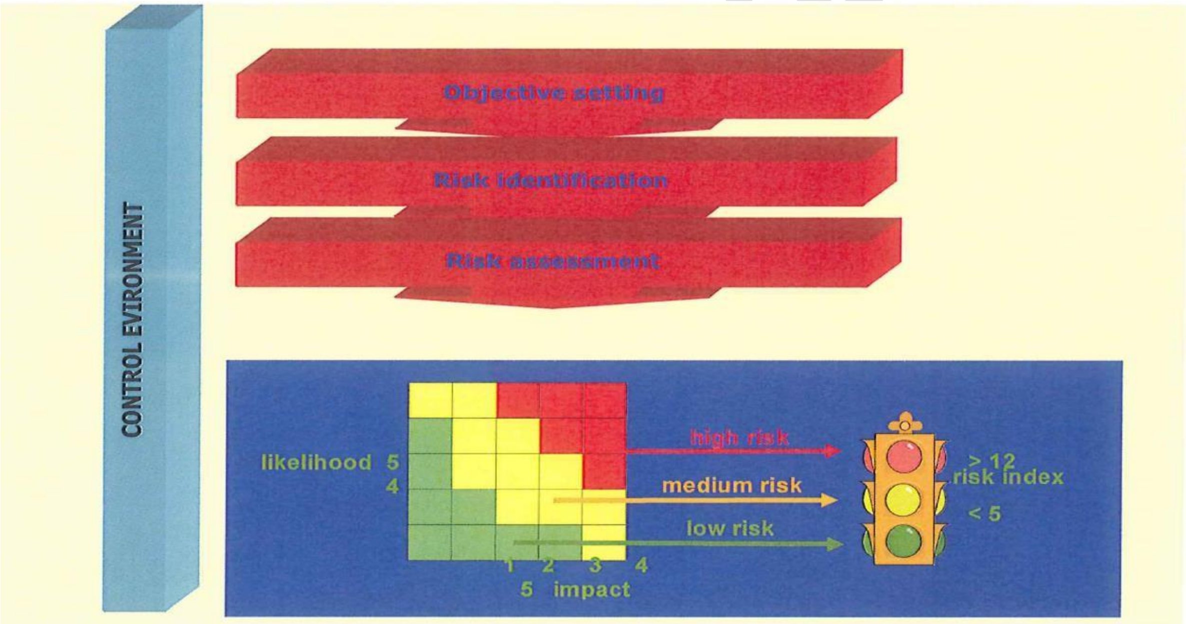
Two main approaches to identify a risk:

a) **Exposures**: The extent of exposure the department is subject to
b) **Environment**: Type of environment which the department is operating under.

Focus on the assets at risk and consider the size, type, probability, and location. Think of who and/ what can be exposed e.g., people, money, assets, intellectual property, business name and reputation, going concern, individual reputation, embarrassment and other. All the above are internal risks for which the department has director control thereupon.

Specific inherent risks: IT covers the following: Competence of employees, Complexity of business environment, adequacy of information systems and activity specific.

9.2 Risk Analysis and Evaluation



The risk analysis process includes five steps:

Step 1: Risk Cause analysis and consequences or impact when that risk materializes. During this stage, management must identify actual events that expose the department to the identified risk. Knowledge of the environment the department is operating in, processes and systems is critical.

Step 2: Quantifying the parameters (scoring system) of impact and the likelihood before the actual assessment; (see example below)

Example impact on cost		
5	Critical	Leads to termination of project
4	Major	Cost increase above 20 percent
3	Moderate	Cost increase above 10 percent

2	Minor	Cost increases less the 10 percent
1`	Insignificant	Minimal or no impact on cost

Example: Certainty of occurrence		
5	Common	Certain to occur, every time
4	Likely	Will occur frequently, 1 out. of 10 times
3	Moderate	Will occur sometimes, 1 out 0f 100 times
2	Unlikely	Will seldom occur, 1 out of 1000 times
1	Rare	Will almost never occur, 1. out of 10 000 times

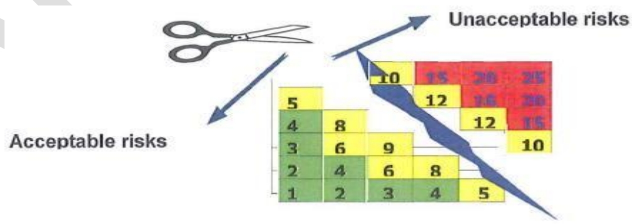
Step 3: Applying the parameters to the risk matrix to indicate what areas of the risk matrix would be regarded as high, medium, or low risk.

Risk magnitude = impact x likelihood

I	**5**	**5**	**10**	**15**	**20**	**25**
M	**4**	**4**	**8**	**12**	**16**	**20**
P	**3**	**3**	**6**	**9**	**12**	**15**
A	**2**	**2**	**4**	**6**	**8**	**10**
C	**1**	**1**	**2**	**3**	**4**	**5**
T		**1**	**2**	**3**	**4**	**5**
				LIKELIHOOD		

	Risk Magnitude
20 – 25	Maximum
15 – 19	High risk
10 – 14	Medium risk
5 – 9	Low risk
1 – 4	Minimum risk

Step 4: Determining the risk acceptance criteria by identifying which risks will not be tolerated.



Step 5: Determine the risk acceptability and what action will be proposed to reduce the risk.

Index	Magnitude	Acceptability	Proposed action
20 -25	Max risk	Unacceptable	Take action to reduce risk with highest priority, accounting officer and executive authority attention.
15 -19	High risk	Unacceptable	
10 -14	Med risk	Unacceptable	Take action to reduce risk, inform senior management
5 – 9	Low risk	Acceptable	No risk reduction – control, monitor, inform management
1 – 4	Min risk	Acceptable	No risk reduction – control, just monitor. and inform management

10 CONTROL SELF ASSESSMENT

10.1 Listing of Controls

Management must list all key control relevant to the risk identified as per root causes analyses. Management must list all key controls relevant to the risk identified as per the root causes analyzed. Those controls will be rated using the same criteria as used with risk rating(estimates).

10.2 Assessment of control for effectiveness

According to your assessment, rate the effectiveness of controls to reduce the risk between **Very Good - Weak** according to how much of the risk the controls reduce. When you subtract the control effectiveness rating from the risk rating, the remainder is your residual risk. The exercise is called the control self-assessment process.

Control effectiveness rating table.

Index	Control Effectiveness	Definition of control adequacy and effectiveness	Risk Management Effective Scale
0%	Non-Existence	Control Activities are inadequate and ineffective and risk exposure are pervasive	No Risk Management. The department lets the risk occur and lives with the results
20%	Weak	Control activities are limited in design adequacy as well as operating effectiveness to mitigate risks exposures. Some of the risk exposure appears to be controlled, but there are. major deficiencies.	Low Risk Management. The risk typically can be detected, but the department relies more on contingency and recovery.
40%	Satisfactory	Control activities are improved in design adequacy and operating effectiveness to mitigate risks exposures. However, there is still room for improvement in certain areas.	Moderate Risk Management. Through effective monitoring, the occurrence of risk is identified and with sufficient time to act and its impact can be reduced, or opportunity is increased.
60%	Good	Control activities are adequately designed and operating effectively to mitigate most key risk exposures	Extensive Risk Management. Ongoing monitoring and initiative-taking activates help and assure the impact of risk occurrence will be minimal or opportunities enhanced.
80%	Very Good	Control Activities are adequately designed and operating effectively to manage and control all key risks. exposures	Continuous Risk Management. A comprehensive risk management programme is in place that helps to ensure that risks are prevented/ there will be no measurable impact on objectives or opportunities are optimized.

After the assessment has been finalized, the risk with high/medium residual values or those that have not been mitigated should be prioritized by risk owners. Action Plans will be developed with deadlines and follow-up dates.

The output of both the risk assessment and control self-assessment is the Risk Register/ risk profile for the Department/District and Local Service Point office/ Section or Unit.

11 Risk management responses or strategies that can be adopted:

11.1 **Risk Avoidance:** This approach simply means that the department does not undertake an activity, action or programme that would produce an undesirable loss exposure.

11.2 **Risk Prevention:** This technique focuses on reducing the frequency of losses. e.g., frequent inspections of an office for overload of electrical outlets are a fire prevention technique.

11.3 **Risk Reduction:** Based on the assumption that it is not feasible, or it is impossible to eliminate or prevent exposure, this method serves to minimize occurrence e.g., the use of sprinkler system will reduce the amount of damage from the fire.

11.4 **Risk Transfer:** Transferring, normally through a contract, the financial and or legal liabilities associated with an identified risk to an outside organization e.g., taking a building lease, as opposed to ownership of a building. Transferring certain risk exposures from the lessee to the lessor or owner of building.

11.5 **Risk Termination:** This technique means that the department stops the activity/processes that gives rise to a particular risk. Termination of the activity in order not to have a loss exposure.

It must be noted that departmental risk appetite/tolerance level will help the department to determine which risk management strategy to use to address a specific risk.

12 OTHER CONTROLS THE DEPARTMENT WILL USE TO MITIGATE RISK

12.1 **Develop concise, written policies and procedures** – the department shall carefully write up-to-date employee policies which will provide a thorough explanation of its rules. Policies and Procedure are the organization's first and best defence against employment-related disputes.

12.2 **Institutes sound general financial management and accounting controls** the creation of adequate accounting controls will focus on authority and approval, proper documentation, physical security and early detection of non-conformance.

12.3 **Institute security safeguards/controls to protect the inadvertent release of confidential information** - these safeguards will include a well thought out security policy, security training and security management and maintenance.

12.4 **Establish ongoing education al programmes -** conduct seminars for staff in such areas as safety, sexual harassment, confidentiality etc. and maintain records of these educational activities.

12.5 **Use a variety of other preventive activities –** such activities will include a client relations programme, an employee newsletter, a formal safety and security programme, a community input effort and ongoing planning, coordination and function review and client surveys (customer feedback)

13 COMMUNICATION AND REPORTING

- Effective and continuous monitoring is an essential part of risk management and therefore relevant. Stakeholders will receive reports pertaining to the status of financial and operational data supported by adequate and appropriate systems. This will be within a time frame that enables staff to carry out their responsibilities properly.

- Awareness campaigns will be detailed together with analysis of previously conducted campaigns, Continuous evaluation of this form of communication will ensure development of campaigns that achieve the desired results.

- Training is another important method of communication where practical skill transfer courses will be upheld on an ongoing basis. Staff will understand what is expected of them and be able to proactively identify, evaluate and implement solutions to risk.

- The reports to top management meetings, Risk management Committee meetings and Audit Committee will provide a balanced assessment of significant risks and effectiveness of risk management process in the department. Any major weakness that has been identified will be noted together with any impact and actions taken to rectify them. It is essential that there be open communication between Chief Risk Officer, Chief Audit Executive, Audit General, Risk Management Committee and Audit Committee

- The Audit Committee will advise what changes, if any, can be made regarding the risk management process. These changes may be due to:

    - Non-achievement of objectives
    - lack of flexibility in responding to changes in the internal and external environment
    - The coverage and quality of the risk management plan
    - Ineffective risk identification, communication, and reporting
    - Commitment of continuous improvement.

14 Monitoring and Review Process

9The monitoring and review process assists in tracking the changes within risk management and the effectiveness of the risk management implementation plan.

Monitoring risks will be linked to the departmental key performance indicators which are in turn linked to the departmental objectives. Senior Management Service Officials will have risk management as key performance indicators in their performance contracts.

15 ROLES AND RESPONSIBILITIES OF ROLE PLAYERS

15.1 RISK MANAGEMENT OVERSIGHT

i. Executive Authority (MEC)

Ensuring that department's strategies are aligned to government mandates.
Obtaining assurance on the management of risks within departments.
Assisting Accounting Officers with management of intergovernmental and political risks
Assisting the Accounting Officers and the departments with the formulation of a Risk Appetite and Tolerance statement

ii. Audit Committee

Oversight of the department's control governance and risk management.
Provide independent and objective views of the department's risk management effectiveness. Audit Committee responsibilities are formally defined in their terms of reference.
Ensuring that internal and external audit plans are aligned to risk profiles of departments.

iii. Risk and Anti-Corruption Committee

Appointed by the Accounting officer to review and ensure the approval of risk policies, including risk appetites and strategies.
Evaluate the extent and effectiveness of integration of risk management within the department.
Evaluate the effectiveness of risk mitigating strategies implemented to address risks.
Exercise control over the functions of other risk-related committees such as OHS Committees; IT Steering Committees; Finance Committees, and these must be streamlined and accounted to Internal Risk Committees.

iv. EC Provincia Treasury

Prescribe uniform risk management norms and standards.
Monitor and assess the department's implementation of the PFMA.
Assist the department in building its capacity for efficient, effective, and transparent risk management.
Enforce the PFMA legislation and any other prescribed norms and standards for risk management in the department.

15.2 RISK MANAGEMENT IMPLEMENTERS

i. Accounting Officer (HOD)

Setting appropriate tone for the effective management of risks within departments.
Delegate responsibilities for the management of risks to senior management/management and other personnel.
Approving risk management policies and Risk Management associated documents.
Providing assurances to relevant stakeholders that key risks are properly identified, assessed, and mitigated.

ii. Senior Management Services Officials

Ensure the identification, management, and monitoring of risks within their area of responsibility and development of risk registers.
Providing risk management progress reports Quartely and annually
Holding officials accountable for their specific risk management responsibilities.

iii. Other officials

Inform their supervisors and/or risk management units of emerging, new risks, and significant changes in known risks.
Co-operate with other role players in the risk management process and provide information as required.
Implement relevant risk mitigation plans through guidance/supervision of business unit leaders/programme managers.

15.3 RISK MANAGEMENT ASSURANCE PROVIDERS

i. Internal Audit

Provide an independent and objective assurance on the effectiveness of the department's system of risk management.
Evaluate the effectiveness of the entire system of risk management and provide recommendations for improvement where necessary.

ii. Auditor General South Africa

Provides an independent opinion on the effectiveness of financial risk management and internal controls.

15.4 RISK MANAGEMENT SUPPORT

i. Chief Risk Officer (Director ORM)

Develop, in consultation with management, departments' risk policies, strategies and implementation plans.
Facilitate risk management training and awareness within the department.
Assist management with the identification, assessment, and monitoring of risks.
Provide Accounting Officers and management with risk intelligence.
Co-operate with other role players in the risk management process and in line with the combined assurance model.

ii. Risk Champions and Coordinators

Function as the focal contact point between the risk manager and the respective Programme or District
Participate in the process of risk identification, analysis, evaluation, and monitoring throughout their programmes.
Assist the program manager in monitoring timeous implementation of program risk mitigating measures.

16. RISK APPETITE AND TOLERANCE LEVELS.

- ✓ The Accounting Officer, Risk and Anti-Corruption Management Committee and the Audit Committee must encourage the taking of controlled risks, the grasping of new opportunities and the use of innovative approaches to further the interests of the Department and achieve its objectives provided the resultant exposures are within the department's risk tolerance range.

- ✓ The Department shall develop a customized risk appetite and tolerance framework that will guide management in which risk can be accepted and those that internal controls must be improved to manage them. This framework must be developed and aligned with the provincial framework developed by the Provincial Treasury.

- ✓ In the absence of the provincial risk appetite and tolerance framework, the department shall adopt the generic risk appetite and tolerance levels set in the Public Sectors Risk Management Framework, limits set by relevant legislation in certain categories (e.g. Zero tolerance on Fraud and OHSA), policies and directives issued from time to time by the National, Provincial government.

- ✓ Operational management and risk management officials will engage in a consultation process to agree on the appropriate risk response for every risk category and every level of risk appetite and risk tolerance during the risk assessment process.

- ✓ Within the department, particular care is needed in taking any action which could:
    - ❖ Impact on the reputation of the department
    - ❖ Impact performance
    - ❖ Undermine the independent and objective review of activities.
    - ❖ Result in censure/fine by regulatory bodies
    - ❖ Result in financial loss

17. DEPARTMENTAL RISK CATEGORIES

The department has adopted the following risk categories, which will be used in all risk assessments conducted within the department:

- ❖ Human resources
- ❖ Knowledge and information management
- ❖ Litigation
- ❖ Loss/theft of assets
- ❖ Material resources (procurement risk)
- ❖ Service delivery
- ❖ Information Technology
- ❖ Third party performance
- ❖ Health & Safety
- ❖ Disaster recovery/ business continuity
- ❖ Compliance/ regulatory
- ❖ Fraud and Corruption
- ❖ Financial
- ❖ Cultural
- ❖ Réputation
- ❖ Economic environment
- ❖ Political environment
- ❖ Social environment
- ❖ Natural environment
- ❖ Technological environment
- ❖ Legislative environment

18. FRAUD PREVENTION PLAN

- ❖ The department, in line with the Public Finance Management Act read with Treasury Regulations and Public Sector Anti-Corruption Strategy, developed a Fraud Prevention Policy and Plan.

- ❖ The purpose of the plan is amongst other things to address fraud and corruption risks that must be addresses and which could jeopardize the successful implementation of each component of the plan.

19. RISK MANAGEMENT IMPLEMENTATION PLAN

- ❖ The department has developed a risk management implementation plan to facilitate the execution of risk management activities and to give an effect on the implementation of the risk management policy and strategy.

20. RISK MANAGEMENT STRATEGY REVIEW AND AMENDMENTS

- ❖ This strategy shall be reviewed three years after the date of approval. However, relevance will be considered on a yearly basis if there are any new developments with the Enterprise-Wide Risk Management environment.

21. RECOMMENDATIONS FOR APPROVAL

Developed by:

____________________________ 25 April 2025
Mr. LB Zenzile (Chief Risk Officer) Date

Recommended / ~~Not Recommended~~ by Chairperson on behalf of the Risk and Anti-Corruption:

____________________________ 29 April 2025
Dr. S. Nyenyiso (Chairperson) Date

Approved /~~Not Approved~~

____________________________ 29/-04/2025
Mr. M Machemba Date
Head of Department