dcstm

Department:
Community Safety and Transport Management
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF COMMUNITY SAFETY AND TRANSPORT MANAGEMENT

RISK MANAGEMENT POLICY
2025/2026

TABLE OF CONTENTS **PAGE**

1. GLOSSARY OF TERMS 4

2. THE PURPOSE 6

3. LEGISLATIVE MANDATE 6

4. SCOPE OF APPLICATION 6

5. RISK MANAGEMENT STATEMENT OF ATTITUDE 6

6. DEFINITION OF ENTERPRISE RISK MANAGEMENT 7

7. BENEFITS OF RISK MANAGEMENT 7

8. RISK MANAGEMENT PROCESS APPROACH 8

9. RISK REPORTING 10
9.1 Risk register 10
9.2 Risk monitoring reports 10

10. ROLES AND RESPONSIBILITIES 10

10.1. IMPLEMENTERS 10
10.1.1. Accounting Officer 10
10.1.2. Management 11
10.1.3. Other Personnel 11

10.2. SUPPORT 11
10.2.1. Risk Management Unit / Chief Risk Officer 11
10.2.2. Risk Champions 11
10.2.3 Co-ordinators 12

10.3. ASSURANCE PROVIDERS 12
10.3.1. Internal Auditors 12

10.4. OVERSIGHT FRAMEWORK 12
10.4.1. Executive Authority 12
10.4.2. Risk Management Committee 13
10.4.4. Audit Committee 13

10.4.5. ICT Strategic Committee 13

11. BUSINESS CONTINUITY AND RECOVERY PLANS 13

12. FRAUD PREVENTION AND RESPONSE PLAN 14

13. COMBINED ASSURANCE POLICY FRAMEWORK 14

14. RISK APPETITE FRAMEWORK 14

15. REVIEW OF THE POLICY 14

16. EFFECTIVE DATE OF THE POLICY 15

17. RECOMMENDATION AND APPROVAL 15

1. GLOSSARY OF TERMS

TERM	DEFINATION
Risk	Any threat, which is currently occurring or has a reasonable chance of occurring in the future, which could undermine achievement of goals and objectives.
Risk Identification	Identification of threats to achievement of goals and objectives.
Risk Assessment	Is a process whereby risks are evaluated to check whether they are high, medium or low by allocating numbers as indicated on the risk management strategy.
Enterprise Risk Management	Is an application of risk management processes within the entire department, instead of only to certain activities or programmes. OR The COSO ERM Framework defines ERM as "the culture, capabilities and practices, integrated with strategy-setting and performance, which organizations rely on to manage risk in creating, preserving and realizing value."18
Executive authority	A member of the executive council who is responsible for the Department of Community Safety and Transport Management.
Accounting Officer	Head of the Department of Community Safety and Transport Management.
Department	Refers to the Department of Community Safety and Transport Management and / or its successor in title.
Control	An existing process, policy, device, practice or other action that acts to minimize negative risk or enhance positive opportunities.
Inherent risk	A risk before taking into consideration the effect of applicable controls.
Likelihood	A general description of probability or frequency
Impact	How the occurrence of the risk will affect the achievement of the set objective.
Monitor	To check, supervise, observe critically or measure the progress of an activity, action or system on a regular basis in order to identify change from the performance level required or expected.
Risk	An unwanted outcome, actual or potential, to the Institution's service delivery and other performance objectives, caused by the presence of risk factor(s). Some risk factor(s) also present upside potential, which Management must be aware of and be prepared to exploit. This definition of "risk" also encompasses such opportunities.
Residual risk	Risk remaining after implementation of risk treatment.

Risk assessment	Overall process of risk identification, risk analysis and risk evaluation.
Risk avoidance	A decision not to become involved in, or to withdraw from, a risk situation.
Risk appetite	The amount and type of risk that the institution is willing to accept in line with its strategic goals. The objective of the Risk Appetite is to indicate the point at which a risk becomes serious enough to the institution to start committing time and effort into the management of the risk.
Risk identification	The process of determining what, where, when, why and how something could happen.
Risk management	A systematic and formalised process to identify, assess, manage and monitor risks.
Risk reduction	Actions taken to lessen the likelihood, negative consequences, or both, associated with a risk.
Risk retention	The acceptance of the burden of loss, or benefit of gain, from a particular risk. It includes the acceptance of risks that have not been identified.
Risk sharing	Sharing with another party the burden of loss, or benefit of gain from a particular risk. It can be carried out through insurance or other agreements.
Risk treatment	A process of selection and implementation of measures to modify risk. Risk treatment measures can include avoiding, modifying, sharing or retaining risk.
Risk tolerance	Risk tolerance is the maximum amount of risk the institution is willing to take for each risk type.
Stakeholders	People and organizations who may affect, be affected by, or perceive themselves to be affected by a decision, activity or risk.
Risk Champion	A person with the skills, knowledge, leadership qualities and power of office required to champion a particular aspect of risk management. Have an understanding of risk management concepts, principles and processes, good analytical skills, expert power, leadership and motivational qualities and good communication skills.
Chief Risk Officer	A senior official who is the head of the risk management unit
Risk Owner	The person accountable for managing a particular risk
Risk Manager	All officials of the department except for the chief risk officer and officials reporting to him/ her.
Governing body	Refers to members charged with governance duties of the Department.
ABBREVIATIONS	
CGICT	Information and Communication Technology Corporate Governance of Information and Communication Technology
ICT	Information and Communication Technology

SANRAL	South African National Road Agency Soc. Ltd
RTMC	Road Traffic Management Cooperation
SACAA	South African Civil Aviation Authority

2. THE PURPOSE

The purpose of this policy is to provide guidance in implementation of the process risk management; and it is intended to relate the Department stance on Risk Management.

3. LEGISLATIVE MANDATE

PFMA Section 38(1) (a) (i) [The Accounting Officer must have and maintain effective, efficient and transparent systems of financial and risk management and internal control.] "
Treasury Regulations: Section 3.2.1: [The Accounting Officer must facilitate a risk assessment to determine the material risks to which the institution may be exposed and to evaluate the strategy for managing these risks.

The Accounting Officer must ensure that a risk assessment is conducted at least annually to identify emerging risks of the institution].

4. SCOPE OF APPLICATION

Risk management process applies to all processes and related activities carried out by all officials at all levels, decision-making activities within the department, including policy development and advice, outsourcing and outsourced services, contract management, front-line service delivery, public events and enabling services.

5. RISK MANAGEMENT STATEMENT OF ATTITUDE

The Department align its risk management policy and strategy with provisions of the Public Sector Risk Management Framework which was adopted by EXCO as the Provincial Framework. The framework guides the implementation of risk management process and cost-effective mitigation of risks to ensure that they are reduced to an acceptable level.

The Department aligns its risk management policy and strategy with provisions of the Public Sector Risk Management Framework which was adopted by EXCO as the Provincial Framework. The framework guides the implementation of risk management process and cost-effective mitigation of risks to ensure that they are reduced to an acceptable level.

It is acknowledged that some risks will always exist and will never be eliminated, however, the Department shall continue to utilise available means to control such risks by reviewing current controls regularly. All employees must understand the nature of risk and accept responsibility for the risks associated with their area of responsibility. The necessary support, assistance and commitment of senior management shall be provided.

The Accounting Officer and Management Committee has a moral and statutory duty to take all reasonable actions to safeguard its employees, assets and the public and ensure that it is not financially or operationally disrupted. It shall meet this duty by ensuring that risk management plays an integral part in the governance processes of the Department.

6. DEFINITION OF ENTERPRISE RISK MANAGEMENT

6.1. Enterprise Risk management is a systematic and proactive process of identifying, evaluating and addressing or managing risks on a continuous basis before such risks can have a negative impact on service delivery *(Public Sector Risk Management Framework)*.

6.2 Risk is about the uncertainty of events, including the likelihood of such events occurring and their effects, both positive and negative, on the achievement of organisation's objectives. Risk includes uncertain events with a potential positive effect on the organisation (i.e. opportunities) not being captured or not materialising.

[King IV Report on Corporate Governance for South Africa]

6.3. Corporate Governance of Information Technology Risks are those risks that may have a negative impact on evaluating and directing the use of Information Communication Technology to support the organisation and monitoring this use to achieve the strategic objectives of the Department.

6.4 ICT risks is defined as direct or indirect loss resulting from inadequate or failed internal processes, people, and systems or from external events. ICT Governance must identify and analyse risks. It should prioritise the risks in terms of likelihood of occurrence and impact, and as result treat them accordingly. The most damaging risks are those, which are not understood.

7. BENEFITS OF RISK MANAGEMENT

The Department acknowledges that it does not operate in a risk free environment and risk management process cannot guarantee such an environment. However, there are benefits that could be derived from the process if implemented effectively. Amongst others;

a. Avoidance/prevention of certain adverse outcomes through taking proactive steps (e.g. fraud risk prevention)
b. Identifying opportunities for continuous improvement
c. Increased probability of achieving objectives
d. Enhancing risk responses by providing the rigour for management to identify alternative risk responses.
e. Reducing operational surprises and losses
f. Identifying and managing multiple and cross-enterprise risks- ERM facilitates coordinated responses to the interrelated impacts and enhances an integrated response to multiple risks.
g. Ensuring proper financial and asset management within the department.
h. Ensuring compliance with laws and regulations
i. Improves the audit outcomes of the Department
j. Increased service availability and quality to ICT users.

8. RISK MANAGEMENT PROCESS APPROACH

The risk management process within the Department takes the approach detailed in the revised/updated COSO framework titled Enterprise Risk Management—Integrating with Strategy and Performance. The framework highlights the importance of considering risk in both the strategy-setting process and in driving performance. It is organized into five easy-to-understand components that accommodate different viewpoints and operating structures, and enhance strategies and decision-making. The five components in the updated Framework are supported by a set of principles. These principles cover everything from governance to monitoring.

Table 1: The table below depicts the 5 ERM components and 20 principles:

Risk management components	Principles	Principles
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	1. Exercises Risk Oversight. 2. Establishes Operating Structures. 3. Defines Desired Culture 4. Demonstrates Commitment to Core Values 5. Attracts, Develops, and Retains Capable Individuals

	Department.	
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 strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.	6. Analyzes Business Context 7. Defines Risk Appetite 8. Evaluates Alternative Strategies 9. Formulates Business Objectives
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.	10. Identifies Risk 11. Assesses Severity/Impact and Likelihood of Risk 12. Prioritizes Risks 13. Implements Risk Responses 14. Develops Portfolio View
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.	15. Assesses Substantial Change. 16. Reviews Risk and Performance. 17. Pursues Improvement in Enterprise Risk Management.

5. Information, Communication, & Reporting	Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the Department.	18. Leverages Information and Technology. 19. Communicates Risk Information. 20. Reports on Risk, Culture, and Performance.

9. RISK REPORTING

9.1 Risk register

The result of the annual risk identification process is reported in the form of both the strategic risk register and operational risk registers. As and when new risks are identified during the course of the year, the registers will be updated with the details of such emerging risks, accordingly.

9.2 Risk monitoring reports

Quarterly progress reports from programme managers on implementation of risk treatment plans as captured on risk registers are submitted to the risk management directorate for compilation of departmental risk monitoring report. The report should be presented to Management, Risk Management Committee and Audit Committee.

10. ROLES AND RESPONSIBILITIES

10.1. IMPLEMENTERS

10.1.1. Accounting Officer

The Accounting Officer is responsible for:

i. Ensuring effective implementation of Risk Management within the Department;
ii. Approves Risk Management policies and strategies;
iii. Provides leadership and guidance for implementation of Risk Management;
iv. Is accountable to the Executive Authority regarding the effectiveness of Risk Management in the Department; and
v. For signing a performance agreement that includes Risk Management, and be appointed in writing by the Executing Authority to indicate the importance of Risk Management.

vi. Intervenes when risk owners are not submitting risk management progress reports or; in cases where risk treatment plans are not making any impact in mitigating the risks.

10.1.2. Management

i. Management as process owners are responsible primarily for risk identification, mitigation and reporting of the progress made on risk mitigation plans.
ii. Management owns the risks, thus taking ownership for management of Departmental risks.
iii. Management are also accountable to the Accounting Officer to integrate the principles of Risk Management in their daily routines to enhance achievement of their service delivery objectives.

10.1.3. Other Personnel

Other personnel are accountable to line management to integrate the principles of Risk Management into their daily routines to enhance achievement of their functional objectives.

10.2. SUPPORT

10.2.1. Risk Management Unit / Chief Risk Officer

i. The Chief Risk Officer provides specialist expertise in providing a comprehensive support service to ensure systematic, uniform and effective ERM;
ii. The Chief Risk Officer plays a vital communication link between operational level management, senior management, Risk Management Committee and other relevant committees;
iii. The Chief Risk Officer is thus the custodian of the ERM Policy, the coordinator of Risk Management throughout the Department and the advisor on all Risk Management matters.

10.2.2. Risk Champions

i. Risk champions are members of the Executive Management Committee at the level of chief director.
ii. Managers within programmes who have managerial and/or specific expertise to deal with certain risks; they are therefore expected to assist in managing risks and are by virtue of their positions regarded as risk champions. Their appointment will therefore not be in writing.
iii. The Risk Champions drive ERM in allocated areas of their responsibilities.
iv. They also add value to risk management process by providing guidance and support to manage 'Problematic' risks and risks of a transversal nature.
v. They also intervene where the risk management efforts are stifled, such as when individuals try to block ERM initiatives.

10.2.3 Co-ordinators

i. Participate in the risk identification and assessment workshops/meeting,

ii. Assist the directorate and/or sub directorates in the implementation of the treatment plans, by evaluating the effectiveness of the mitigating strategies to address the material risk of the Department.

iii. Report to Risk management and risk owners of any material changes to the risk profile or identification of emerging risks.

iv. Co-ordinate submission of monthly progress reports on implementation of risk treatment plans to Risk management unit.

10.3. ASSURANCE PROVIDERS

10.3.1. Internal Auditors

Internal Auditors are responsible for providing independent assurance on the effectiveness of Risk Management in the Department. This involves providing assurance that all material risks have been identified and assessed and that control systems implemented to treat such risks are both adequate and effective.

10.3.2. Auditor General

The Auditor-General is responsible for providing an opinion on:

i. The reasonability of the financial statements of the Department; and
ii. Compliance with applicable legislation.

In addition, the Auditor-General is required to highlight weaknesses or deficiencies in the performance reporting of the institution. In providing an opinion on compliance with legislation, the Auditor-General shall also provide independent assurance on the effectiveness of the Risk Management activities of the Department.

10.3.3 Other regulatory bodies

Regulatory bodies relevant to the Department include Office of Premier, Provincial Legislature and Treasury, SANRAL, RTMC, SACAA etc. They provide assurance on compliance to relevant legislation.

10.4. OVERSIGHT FRAMEWORK

10.4.1. Executive Authority

The Executive Authority is accountable to the Legislature to ensure attainment and achievement of goals and objectives of the Department. In this context, the Executive Authority should take an interest in ERM to the extent necessary to obtain comfort that properly established and functioning systems of Risk Management are in place to protect the Department.

10.4.2. Risk Management Committee

Risk Management Committee is responsible for the oversight of the quality, integrity and reliability of the Risk Management processes and risk responses and shall be appointed in writing by the Accounting Officer.

An important part of the Committees mandate is to provide recommendations to the Accounting Officer to continuously improve management of specific risks as well as the overall process of Risk Management and to ensure that ICT risks are adequately managed.

10.4.3. Provincial Risk Management Support

Provincial Treasury has specific duties to provide an oversight on implementation of risk management activities within the Department.

10.4.4. Audit Committee

In terms of the Treasury Regulations 3.1.10 (c) and 3.2.7 (a), the Audit Committee is responsible for assisting the Accounting Officer in addressing its oversight requirements of Risk Management and evaluating and monitoring the Department's performance concerning Risk Management. This Committee must work in partnership with the ICT Strategic Committee, on major ICT risks and performance measurement.

10.4.5. ICT Strategic Committee

This Committee must work in partnership with the other departmental committees (Risk Management Committee, Audit Steering Committee etc.) and Management to provide input to, review and amend the aligned corporate and ICT strategies. The roles of the committee are:

i. To monitor the management of ICT related risks;
ii. Monitoring of risk and return on ICT investment;
iii. Monitoring progress on major mission critical risks to ICT projects;

11. BUSINESS CONTINUITY AND RECOVERY PLANS

Business Continuity and Recovery Plans are the most critical strategies of dealing with risks that occurs seldom but with disastrous consequences, such risks could result in business shutdowns and disasters.

The Department is in the process of finalisation of business continuity planning and recovery plans. The plans are intended to provide guidance to the employees on what actions to be taken during disaster and how quick services could be restored.

12. FRAUD PREVENTION AND RESPONSE PLAN

The Department has a policy and a strategy on Anti-corruption, ethics and integrity management in place, measures are intended to prevent and detect unethical behaviour that prevailed within. Monitoring of implementation of the strategy is performed regularly and reporting thereof is done to management and relevant stakeholders.

13. COMBINED ASSURANCE POLICY FRAMEWORK

The Department has developed a combined assurance policy framework in order to integrate and align assurance processes for maximised risk governance. The policy framework aims to provide guidance, in a simple manner, on the effectiveness of assurance providers and to create confidence in the assurance provided over key departmental risks.

14. RISK APPETITE FRAMEWORK

a. The objective of the risk appetite framework is -

i. To provide Management with guidance on the levels of risk that are legitimate for them to take, or not and seize important opportunities that have potential to improve service delivery.

ii. It also seeks to demystify the notion of risk appetite in order to encourage and steer the course where risk taking is clearly calculated with a view to achieving defined rewards.

b. Over-arching risk appetite statement.

Department strives to maintain a low appetite for risk; however, it is acknowledging that in pursuit of the mandate at times activities that inherently carry greater risks may be undertaken. Where the Department chooses to accept an increased level of risk it will do so, subject always to ensuring that the potential benefits and threats are fully understood before actions are authorised, that it has sufficient risk capacity, and that sensible and proportionate measures to mitigate risk are established.

15. REVIEW OF THE POLICY

This policy shall be reviewed annually or as and when it is deemed necessary to reflect any changes that may occur in the Department.

16. EFFECTIVE DATE OF THE POLICY

This policy shall take effect immediately after the Accounting Officer has approved.

17. RECOMMENDATION AND APPROVAL

DISCUSSED AND ADOPTED DURING	DATE
DEPARTMENTAL MANAGEMENT COMMITTEE	25 / 03/2025
RISK MANAGEMENT COMMITTEE	26 / 03 /2025

RECOMMENDED

MR. A KYEREH
CHAIRPERSON
DATE: 27 / 03 /2025

APPROVED

DR. HANS KEKANA
HEAD OF DEPARTMENT
DATE: 31 / 03 /2025