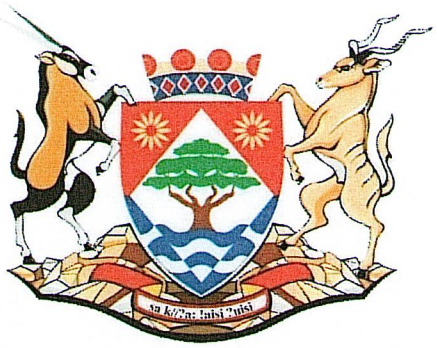

the dr&pw

Department:
Roads and Public Works
NORTHERN CAPE PROVINCE
REPUBLIC OF SOUTH AFRICA

DEPARTMENTAL POLICY ON RISK MANAGEMENT

Version 4

(August 2023)

TABLE OF CONTENTS

Contents Page

1. DEFINITIONS AND ACRONYMS

"AG"	Means Auditor General. The Office of the Auditor General is an institution of state, established by Chapter 9 of the Constitution of the Republic of South Africa, 1996. The AG also functions in terms of the Public Audit Act, 2004 (Act No. 25 of 2004) and as amended by the Public Audit Amendment Act, 2018 (Act No. 5 of 2018). As an oversight body responsible for overseeing the management of public finances on behalf of the parliament/provincial legislatures, the functions of the AG are to ascertain, investigate and audit all the accounts and financial statements of: a) all departments of the national, provincial and local spheres of the government; and b) any statutory body or any other institution which is financed wholly or partly by public funds, including public corporations, parastatals and other entities. Besides conducting performance audits, once public expenditure of departments have been audited, the AG prepares and publishes a report for that particular public institution. The report is then submitted to parliament/provincial legislature for discussion. The AG is basically the extension of the legislature's committees, including the Standing Committee on Public Accounts (SCOPA), in that they use the very report of the AG to summon whoever they wish to summon, particularly the Accounting Officers (AOs) and Political Heads (MECs) of departments. Accounting Officers refer to the highest ranking administrative officials who head a state department or municipality or any other public sector institution, inclusive of parastatals and public corporations. Accounting Officers are directly accountable to parliament or a relevant Provincial Legislature in respect of their performance, particularly financial matters. Parliament and every Provincial Legislature have a SCOPA, which summon Accounting Officers to give an account of financial transactions involving their specific institutions.
"AO"	Means Accounting Officer, which refers to a person mentioned in section 36 of the Public Finance Management Act (PFMA), 1999 (Act No. 1 of

	1999), as amended. The AO is also the Head of Department (HOD).
"CAE"	Means Chief Audit Executive, which refers to the Senior Management Service (SMS) official who is responsible for Internal Audit activities in the DR&PW (where Internal Audit activities are sourced from external providers, the Chief Audit Executive is the person responsible for overseeing the service contract and the overall quality of the service provider).
"CRO"	Means Chief Risk Officer, which refers to the Senior Management Service (SMS) official who is responsible for the management of Risk in the DR&PW.
"Corruption"	Refers to the unlawful and intentional making of a misrepresentation which causes actual prejudice or which is potentially prejudicial to another.
"Department/ DR&PW"	Means Department of Roads and Public Works, Province of the Northern Cape.
"ERM"	Means Enterprise Risk Management. ERM can be defined as a process, implemented by the departmental Management and personnel, applied in strategy setting and across the operations of the Department, designed to identify potential events that may affect the DR&PW and manage risk to be within the departmental Risk Appetite, in order to provide reasonable assurance regarding the achievement of departmental objectives.
"ERP"	Means Ethics Risk Profile, which represents a particular type of risk profiling and which forms part of the general departmental Risk Profile. The objective with compiling an ERP is the management of organisational integrity and thus to build an ethical corporate culture within the DR&PW. The Department builds an ethical culture in a formal way by, amongst others, compiling an annual Ethics Risk Profile, implementing a Code of ethical conduct; integrating Ethical Standards into work processes and procedures; and reporting on and disclosing the Ethics Performance of the DR&PW.

"Executive/Executing Authority (EA)"	The Executing/Executive Authority refers to the Member of the Executive Council (MEC) of the Province of the Northern Cape, who is responsible for a department, in this case the Department of Roads and Public Works (DR&PW), as defined in section 1(1) of the Public Service Act, 1994 (Act No. 103 of 1994), as amended, except with regard to the appointment and other career incidents of a Head of Department (HOD), in which case it means the Executing Authority as contemplated in section 3B of the abovementioned Act. The MEC is also accountable to the Northern Cape Provincial Legislature (NCPL).
"FPERC"	Means Fraud Prevention, Ethics and Risk management Committee, a departmental sub-committee of the DR&PW, which replaces the previous Joint Risk Management Committee (JRMC). The FPERC is appointed by the Accounting Officer to, amongst others; review the Department's system of risk management. The FPERC is a sub-committee of the DR&PW's Internal Audit Committee (IAC).
"Fraud"	Fraud refers to a deception that is intentional and caused by an employee/network of employees for personal gain. In other words, fraud is a deceitful activity used to gain an advantage or generate an illegal profit.
"IAC"	Means Internal Audit Committee, which is an independent committee constituted to, amongst others, review the control, governance and risk management within the DR&PW, established in terms of section 77 of the PFMA. According to section 38(1)(a)(ii) of the PFMA, 1999, as amended, the accounting officer for a Department, trading entity or constitutional institution must ensure that *"a system of internal audit under the control and direction of an audit committee complying with and operating in accordance with regulations and instructions prescribed in terms of sections 76 and 77"* is established and maintained.
"ICT"	Means Information and Communication Technology.
"Inherent Risk"	Refers to the exposure arising from risk factors in the absence of deliberate management intervention(s) to exercise control over such factors.

"Internal Auditing"	Refers to an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.
"King II and III"	Refer to the King Reports on Corporate Governance in South Africa for 2002 and 2009 respectively. The King Committee on governance issued the *King Report on Governance for South Africa – 2009 (the "Report")* and the *King Code of Governance Principles – 2009 (the "Code")*, together referred to as *"King III"* on 1 September 2009. The issuance of King III was necessitated by, at the time, the new Companies Act of 2008 and changes in international governance trends since the release of the second King Report on Corporate Governance for South Africa (King II) in 2002.
"Management"	Means all officials of the Department except the Chief Risk Officer and officials reporting to him/her.
"M&E"	Means Monitoring and Evaluation.
"MISS"	Refers to the Minimum Information Security Standards Policy of the South African Government, as approved by Cabinet.
"NCPT"	Means Northern Cape Provincial Treasury.
"Other Official"	Means an official other than the Accounting Officer, Management, the Chief Risk Officer and his/her staff.
"PFMA"	Means Public Finance Management Act, 1999 (Act No.1 of 1999), as amended by Act No.29 of 1999.
"PAIA"	Means Promotion of Access to Information Act, 2000 (Act No. 2 of 2000).
"PAMA"	Means Public Administration Management Act, 2014 (Act No. 11 of 2014).

"PDA"	Means Protected Disclosures Act, 2000 (Act No. 26 of 2000).
"PIA"	Means Protection of Information Act, 1982 (Act No. 84 of 1982).
"POCA"	Means Prevention of Organized Crime Act, 1998 (Act No. 121 of 1998).
"PRECCA"	Means Prevention and Combating of Corrupt Activities Act, 2004 (Act No. 2 of 2004).
"PSA"	Means Public Service Act, 1994 (Act No. 103 of 1994).
"PSCBC"	Means Public Service Coordinating Bargaining Council.
"PSRMF"	Means Public Sector Risk Management Framework (PSRMF).
"Residual Risk"	Refers to 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).
"Responding to Risk"	Risk response is concerned with the development of strategies to reduce or eliminate the threats and events that create risks.
"Risk"	Refers to 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 the DR&PW Management must be aware of and be prepared to exploit. This definition of "risk" also encompasses such opportunities, which are also called "risk optimisation".
"Risk Appetite"	Refers to the amount and kind of residual risk that the Department is *willing* to accept.
"Risk Assessment"	Refers to a systematic process to quantify or qualify the level of risk associated with a specific threat or event, in order to enrich the Risk Intelligence available to the Department.

"Risk Champion"	Refers to a person (i.e. Deputy Director or Assistant Director) who, by virtue of his/her expertise or authority, champions a particular aspect of the Risk Management Process, but who is **not** the Risk Owner.
"Risk Evaluation"	Refers to the process of comparing the estimated risk against given risk criteria to determine the significance of the risk. Risk evaluation may be used to assist in the decision to accept or to treat a risk.
"Risk Financing"	Refers to the allocation of budgeted funds in order to meet the cost of implementing Risk Treatment and related costs (inclusive of the financial consequences related to particular risks) of the DR&PW.
"Risk Factor"	Refers to any threat or event which creates, or has the potential to create risk.
"Risk Identification"	Refers to a deliberate and systematic effort to identify and document the Department's key risks for a particular pre-determined time frame, e.g. a financial year.
"Risk Management"	Refers to a systematic and formalised process to identify, assess, manage and monitor departmental risks. Risk management is the identification and evaluation of actual and potential risk areas as they pertain to the DR&PW as a total entity, followed by a process of either avoidance, termination, transfer, tolerance (acceptance), exploitation, or mitigation (treatment) of each risk, or a response that is a combination or integration. Accountability for proper Risk Management rests with the Executive Management of the DR&PW, which fulfils the role of a Board of Directors, compared to a private company. Every employee in an organization however, has responsibility for risk management. Risk management therefore has to be fully integrated into the daily operations of the Department.
"Risk Management Process"	The Risk Management Process entails the planning, arranging and controlling of activities and resources to minimise the negative impacts of all risks to levels that can be tolerated by stakeholders whom the departmental Management has identified as relevant to the business of

	the DR&PW, as well as to optimise the opportunities, or positive impacts, of all risks.
"Risk Mitigation"	Means the limitation of any negative consequence(s) of a particular event.
"Risk Management Unit"	Refers to a business unit of the DR&PW that is responsible for coordinating and supporting the overall departmental Risk Management Process, but which does not assume the responsibilities of the Department's Management for identifying, assessing and managing risks.
"Risk Optimisation"	Refers to a process related to a risk, in order to exploit the risk opportunities, minimise the negative and to maximise the positive consequences and their respective probabilities.
"Risk Perception"	Refers to the way in which a stakeholder views a risk based on a set of values or concerns. Risk perception depends on the stakeholder's needs, concerns and knowledge. Risk perception is subjective and can differ from objective evidence and data.
"Risk Profile"	The DR&PW and its District Offices, in terms of its functional areas, has an inherent and residual Risk Profile. These are all the risks faced by the Department, ranked according to a risk matrix and indicated graphically on a matrix. The Risk Score may be determined by multiplying the frequency and severity of the risks, where these are indicated. The departmental Risk Profile is reviewed annually and includes an Ethics Risk Profile (ERP).
"Risk Owner"	Refers to the DR&PW officials who are *accountable* for managing a particular risk, i.e. Chief Directors and Senior Managers.
"Risk Register"	Refers to a formal listing of risks identified, together with the results of the Risk Analysis and Risk Evaluation procedures, in conjunction with the details of Risk Treatment, Risk Control and Risk Reduction and Mitigation Plans.

"Risk Response"	Refers to the process of selection and implementation of measures to modify risk. The term "risk treatment" is sometimes used for the measures themselves. Risk response measures can include treating, avoiding, optimising, transferring, terminating or retaining risk.
"Risk Retention"	Refers to the acceptance of the burden of loss, or benefit of gain, from a particular risk. Risk retention includes the acceptance of risks that have not been identified. There can be variability in the degree of acceptance and dependence on risk criteria.
"Risk Tolerance"	Refers to the amount and kind of risk the Department is *capable* of tolerating (as opposed to the amount and kind of risk the Department is *willing* to tolerate).
"Risk Transfer"	Means sharing with another party the burden of loss or benefit of gain, for a risk. Legal or statutory requirements can limit, prohibit or mandate the transfer of certain risk. Risk transfer can be carried out through agreements such as Memorandums of Agreement and Memorandums of Understanding. Risk transfer can create new risks or modify existing risk. Relocation of the source of risk is not risk transfer.
"SAPS"	Means South African Police Service.
"WPA"	Means Witness Protection Act, 1998 (Act No. 112 of 1998).

2. INTRODUCTION

2.1 This policy seeks to outline the Department's commitment to protecting the DR&PW against adverse outcomes which may impact negatively on Service Delivery.

2.2 This policy further seeks to confirm the Department's commitment to the established legal and regulatory framework for risk management in South Africa.

2.3 The DR&PW Management will, by means of these policy guidelines implement a comprehensive system of controls to ensure that risks are mitigated and that the DR&PW's objectives are attained.

2.4 The aforementioned controls must create an environment which will set the tone for risk management in the Department and also cover ethical values, Management's service delivery philosophy and the competence of employees.

2.5 Any vulnerability in the achievement of the DR&PW's objectives, whether caused by internal or external risk factors, must be detected in good time and reported by the systems of control in place and met with appropriate interventions. This course of action will not only improve the DR&PW's Risk Profile and thereby enhance the Department's Service Delivery Vision and Mission, but it will also enhance any possible positive influences of risk on the Department.

2.6 It must be borne in mind that risk management processes and the review thereof may identify areas of opportunity, such as where effective and efficient risk management can be turned into an advantage for the Department. Risk management should therefore not only be viewed from a negative perspective.

2.6 The DR&PW hereby recognise that risk management goes beyond the control of financial risks. The reputation of the Department and its future are also at stake.

2.7 The DR&PW must therefore ensure that the governance surrounding risk management in the Department is transparent and appropriately disclosed to its stakeholders in government e.g. the AG and the Provincial Legislature; and outside of government e.g. to our citizenry, communities and the wider public.

2.8 DR&PW officials must be aware of the fact that risk management is a continuous process of identifying, evaluating and managing risk. If staff members of the Department do not see risk management as more than just an act of compliance, the Department is unlikely to reap the benefits it can offer.

3. OBJECTIVES

The objectives of this policy are to:

3.1 ensure that every effort is made within the Department to manage risks within the prescribed legal and other relevant regulatory frameworks;

3.2 maximise potential opportunities in terms of risk optimisation and minimise the adverse effects of risks on the DR&PW;

3.3 promote the adoption of sound Risk Management Practices within the Department;

3.4 assist the Department's Management in decision making;

3.5 improve accountability, efficiency and effective administration within the Department;

3.6 promote a DR&PW-wide Risk Management Culture and to improve risk transparency to the DR&PW's stakeholders;

3.7 maximise the departmental stakeholders' value (including value for money) by managing risks that may impact negatively as defined by the financial and performance drivers of the DR&PW;

3.8 assist the Department in enhancing and protecting those opportunities that presents the greatest service delivery benefits; and

3.9 address the DR&PW's exposure to:

a) physical and operational risks;
b) human resource risks;
c) technical risks;
d) business continuity and disaster recovery;
e) credit and market risks;
f) ethics risks; and
g) compliance risks.

4. REGULATORY FRAMEWORK

The following instruments provide the legal framework for the responsibilities of the DR&PW Management, as well as the responsibilities of Other Officials of the Department in terms of departmental risk management, namely:

4.1 The Constitution of the Republic of South Africa, 1996.

4.2 The Public Finance Management Act (PFMA), 1999 (Act No.1 of 1999), as amended by PFMA Amendment Act, 1999 (Act No. 29 of 1999), specifically sections 38, 39, 40, 41 and 45, as it applies to risk management and internal control.

4.3 The Prevention and Combating of Corrupt Activities (PRECCA) Act, 2004 (Act No. 2 of 2004), which aims to prevent and fight corruption in the Public Sector, Government in general, as well as in the Public Administration.

4.4 The Prevention of Organized Crime Act (POCA), 1998 (Act No. 121 of 1998).

4.5 The Promotion of Access to Information Act (PAIA), 2000 (Act No. 2 of 2000) and the PAIA Manual.

4.6 The Protection of Information Act (PIA), 1982 (Act No. 84 of 1982).

4.7 The Witness Protection Act (WPA), 1998 (Act No. 112 of 1998).

4.8 Section 2(1) (a) & (b) of the Protected Disclosures Act (PDA), 2000 (Act No. 26 of 2000).

4.9 The Public Administration Management Act (PAMA), 2014 (Act No. 11 of 2014).

4.10 The Public Service Act (PSA), 1994 (Act No. 103 of 1994).

4.11 The Public Service Anti-Corruption Strategy, 2000.

4.12 The Public Service Anti-Corruption Strategy, 2002.

4.13 The National Anti-Corruption Strategy, 2020-2030.

4.14 National Treasury Regulations, 2001, 2005 and Guidelines.

4.15 The King II Report on Corporate Governance, 2002.

4.16 The King III Report on Corporate Governance, 2009.

4.17 The Batho Pele Principles.

4.18 The Public Sector Risk Management Framework, 2010.

4.19 The Public Service Regulations (PSR), 2001, as amended in 2002 and 2016.

4.20 The Disciplinary Code and Procedure for the Public Service (PSCBC Resolution 2 of 1999).

4.21 The Code of Conduct for the Public Service, as contained in the Public Service Regulations, 2016.

4.22 The Minimum Information Security Standards (MISS) policy as approved by Cabinet on 04 December 1996, as amended.

4.22 The following associated departmental regulatory frameworks, amongst others, apply:

a) The DR&PW Policy on Damages and Losses.
b) The DR&PW Risk Management Strategy.
c) The DR&PW Monitoring and Evaluation (M&E) Policy Framework.
d) The DR&PW Policy on Irregular Expenditure.
e) The DR&PW Policy on Fruitless and Wasteful Expenditure.
f) The DR&PW Policy on Unauthorised Expenditure.
g) The Current DR&PW Internal Audit Plan.
h) The Plan: DR&PW Compilation of Policies on Fraud, Corruption and Ethics Management, specifically the following:
    (i) the DR&PW Anti-Fraud and Corruption Implementation Plan;
    (ii) the DR&PW Anti-Fraud and Corruption Charter;
    (iii) the DR&PW Code of Ethics and Conduct;
    (iv) the DR&PW Anti-Fraud and Corruption Policy and Response Plan;
    (v) the DR&PW Anti-Fraud, Anti-Corruption and Ethics Strategy;
    (vi) the DR&PW Terms of Reference of the departmental Fraud Prevention, Ethics and Risk management Committee (FPERC);
    (vii) the DR&PW Policy on Whistle Blowing / Protected Disclosures; and
    (viii) the DR&PW Whistle Blowing / Protected Disclosures Guidelines.

5. SCOPE AND APPLICATION

5.1 The realisation of strategic objectives demands from the Department to take calculated risks in a way that does not jeopardise the direct interests of the stakeholders. Sound management of risk will

enable the Department to anticipate and respond to changes in the service delivery environment, as well as make informed decisions under conditions of uncertainty.

5.2 The principles in this policy will apply to all employees of the Department whether appointed on permanent or temporary/contract basis as well as to officials enrolled in the internship/learnership programmes.

5.3 Furthermore this policy will be applied in all the activities of the Department.

5.4 Risk Management must be incorporated into the performance agreements and job descriptions of management.

5.5 As prescribed, the performance agreement or work plans of the Department's managers will provide for the Core Management Criteria of "People Management" which hold managers accountable for addressing misconduct and fraud within their sections.

6. ROLES AND RESPONSIBILITIES

The following persons are responsible for the management of risk within the Department, namely:

6.1 The Executive/Executing Authority (MEC)

The responsibilities of the Executive Authority or Member of the Executive Council (MEC) for Roads and Public Works in the Province of the Northern Cape, with regards to risk management are to:

a) ensure that the Department's strategies are aligned to its government mandate;
b) obtain assurance from management that the Department's strategies were identified and assed, and are properly managed;
c) assist the Accounting Officer (HOD) to deal with fiscal, intergovernmental, political and other risks which are beyond his/her direct control and influence;
d) insist on the achievement of objectives, effective performance management and add value for money;
e) raise awareness of and concurring with the Department's risk appetite and tolerance levels;
f) provide oversight over the Department's portfolio of risks and consider it against the Department's risk tolerance;
g) require that Management should have an established set of values by which every employee should abide by;
h) insist on accountability; and

i) create an enabling environment to ensure that the institutional environment of the Department supports the effective functioning of risk management.

6.2 The Accounting Officer (AO)

The responsibilities of the AO, who is also the Head of Department (HOD) with regard to risk management, are to:

a) set the tone at the top by supporting Enterprise Risk Management (ERM) and allocating resources towards the implementation thereof;
b) establish the necessary structures and reporting lines within the Department to support ERM;
c) approve the Risk Management Strategy, Risk Management Policy, Risk Management Implementation Plan and Fraud, Corruption and Ethics Management Policies of the Department;
d) approve the Department's Risk Appetite and Risk Tolerance Policy;
e) influence and compel the Department to have a risk "awareness" culture;
f) approve the Department's Code of Ethics and Conduct and hold Management and Officials accountable for its adherence;
g) hold Management accountable for designing, implementing, monitoring and integrating risk management principles into their day–to–day activities;
h) ensure that a conducive control environment exists to ensure that identified risks are proactively managed;
i) leverage the Internal Audit Committee (IAC), the Directorate Internal Audit, the Fraud Prevention, Ethics and Risk management Committee (FPERC) and other appropriate departmental structures to improve the overall state of risk management in the DR&PW;
j) provide appropriate leadership and guidance to Senior Management Service (SMS) members and structures responsible for various aspects of risk management.

6.3 The Fraud Prevention, Ethics and Risk management Committee (FPERC)

6.3.1 The responsibilities of the FPERC with regard to risk management in terms of this policy are to:

a) Review and recommend for approval of the Accounting Officer the DR&PW's Risk Management Policy, Risk Management Strategy, Risk Management Implementation Plan and the Department's Policy on Risk Appetite and Tolerance, ensuring that limits are:
   i. supported by a rigorous analysis and expert judgement;
   ii. expressed in the same values as the Key Performance Indicators (KPIs) to which they apply;

iii. set for material risks individually, as well as in aggregate for particular categorisation of risk; and

iv. consistent with the Materiality and Significance Framework, the FPERC must take responsibility for:

- ✓ The Department's ability to withstand significant shocks.
- ✓ The Department's ability to recover financially and operationally from significant shocks.
- ✓ Evaluate the extent and effectiveness of integration of risk management within the Department.
- ✓ Assess the implementation of the DR&PW's Risk Management Policy, Risk Management Strategy, Risk Management Implementation Plan and the Department's Policy on Risk Appetite and Tolerance.
- ✓ Evaluate the effectiveness of the mitigating strategies implemented to address the material risks of the Department based on the departmental Risk Profile, inclusive of the Ethics Risk Profile (ERP) of the DR&PW and taking into account the departmental Risk Register.
- ✓ Review the material findings and recommendations by assurance providers on the departmental system of risk management and monitor the implementation of such recommendations.
- ✓ Develop its own Key Performance Indicators (KPIs) for approval by the AO.
- ✓ Report to, and interact with the IAC, to share information relating to material risks of the Department.
- ✓ Provide timely and useful reports to the AO on the state of risk management in the Department, together with accompanying recommendations to address any deficiencies identified by the FPERC and IAC.

6.3.2 In instances where the scale, complexity and geographical dispersion of the Department's risk management activities dictate the need for the FPERC to work through sub–committees, the FPERC must ensure that:

a) approval is obtained from the AO for the establishment of such sub–committees;
b) the Terms of Reference of the sub–committees are aligned to that of the FPERC; and
c) the FPERC exercises effective control over the functioning of the sub–committees.

6.4 The Chief Risk Officer (CRO)

The responsibilities of the CRO with regard to risk management in the DR&PW are to:

a) Work with Senior Management to develop the Department's vision for risk management.

b) Develop, in consultation with Management, the Department's Risk Management Framework (RMF) incorporating, inter alia, the following:
   i. DR&PW Risk Management Policy;
   ii. DR&PW Risk Management Strategy;
   iii. DR&PW Risk Management Implementation Plan and Risk Management Methodology;
   iv. Risk Appetite and Tolerance Policy of the Department;
   v. the Risk Profile, inclusive of the Ethics Risk Profile (ERP) of the DR&PW;
   vi. the departmental Risk Register;
   vii. Risk Financing Recommendations, which include incurred or probable costs of risk associated with, amongst others, the following:
      ✓ self retained losses (incurred loss);
      ✓ risk control expenses including safety, security, property conservation and quality control programs, etc.;
      ✓ maintenance costs;
      ✓ machinery breakdown costs;
      ✓ consulting charges;
      ✓ training costs;
      ✓ administrative costs, including general risk management and risk management consulting costs;
      ✓ outside claims and loss control services;
      ✓ costs associated with losses as a result of fraud and corruption.
   viii. Risk Classification within the Department.

c) Communicate the Department's Risk Management Framework (RMF) to all stakeholders in the Department and monitor its implementation.
d) Facilitate orientation and training for the FPERC regarding risk management.
e) Training stakeholders in their risk management functions.
f) Continuously driving risk management to higher levels of maturity.
g) Assist management with risk identification, assessment and development of response strategies.
h) Monitor the implementation of response strategies.
i) Collate, aggregate, interpret and analyse the results of risk assessment to extract intelligence for proper, effective and efficient departmental responses.
j) Report risk intelligence to the AO and the FPERC.
k) Cooperate with Internal Audit, Management and the AG in developing the combined Assurance Plan for the Department.

6.5 The DR&PW Management

The responsibilities of the departmental Management, which includes Senior Management Service (SMS) and Middle Management Service (MMS) members with regard to risk management, are to:

a) Execute their responsibilities in the departmental Risk Management Policy and Risk Management Strategy.
b) Empower officials under their control to perform effectively in their risk management responsibilities through communication of responsibilities, comprehensive orientation and ongoing opportunities for skills development.
c) Align the functional risk management methodologies and processes with the Department's management processes.
d) Devoting personal attention to overseeing the management of Key Risks within their area of responsibility.
e) Maintain a cooperative relationship with the FPERC and other relevant Risk Owners and Risk Champions in the Department.
f) Provide Risk Management Reports as required.
g) Present to the FPERC and the IAC information as requested.
h) Maintain proper risk control within their area of responsibility. Five (5) essential aspects of control within each area of responsibility are identified, namely:
    i. proper functioning of the control environment;
    ii. risk assessment;
    iii. control activities;
    iv. risk information and communication; and
    v. monitoring and evaluation regarding risks and the management thereof.
i) Hold officials accountable for their specific risk management responsibilities.

6.6 Other Officials

The responsibilities of Other Officials with regard to risk management in the DR&PW are to:

a) Apply the appropriate departmental risk management processes in their respective functions.
b) Implement the delegated Action Plans to address identified departmental risks.
c) Inform their supervisors and/or the departmental Risk Management Unit of new risks and significant changes in known risks.
d) Cooperate with other relevant role players in the risk management process and providing information as required.
e) Report suspicion of fraud and/or corruption to the CRO and Management.
f) Report inefficient, unnecessary or unworkable controls.

g) Participate in Risk Identification and Risk Assessment within their respective departmental business units.
h) Adhere to the Code of Ethics and Conduct of the DR&PW, as well as the Public Service Code of Conduct.
i) Act within the Risk Appetite and Risk Tolerance levels set by their particular business unit.
j) Familiarise themselves with the overall risk management Vision, Risk Management Policy and Risk Management Strategy of the Department, as well as the DR&PW Policies regarding Fraud, Corruption and Ethics Management.

6.7 Risk Champions

The responsibilities of Risk Champions with regard to risk management in the Department are to:

a) Intervene and, where necessary, escalate matters in instances where the departmental risk management efforts are being hampered for example, by the lack of cooperation by Management and Other Officials and the lack of institutional skills, expertise, and necessary human and financial resources.
b) Add value to the DR&PW's risk management process by providing guidance and support to manage "problematic" risks and risks of a transversal nature that require a multiple participant approach.
c) Act as Change Agents in the DR&PW's risk management process, a role that is distinguished from that of Risk Owners because Risk Champions are trouble shooters that facilitate resolution of risk related problems.
d) Assist the Risk Owners to resolve risk related problems.

6.8 Internal Audit

6.8.1 The responsibilities of Internal Audit with regard to risk management in the DR&PW are to:

a) Provide an independent, objective assurance on the effectiveness and efficiency of the Department's system of risk management.
b) Evaluate the effectiveness and efficiency of the entire system of departmental risk management and provide recommendations for improvement, where necessary.
c) Develop an Internal Audit Plan for the DR&PW on the basis of Key Risk Areas in terms of the International Standards for the Professional Practice of Internal Audit.
d) Determine whether departmental risk management processes are effective and efficient, which is a judgement resulting from the Internal Audit Auditor's assessment of whether:
   i. the DR&PW's objectives support and align with the departmental vision and mission;
   ii. significant departmental risks are identified and assessed;
   iii. risk responses by the DR&PW are appropriate to limit risk to an acceptable level; and

iv. relevant departmental risk information is captured and communicated in a timely manner to enable the AO, the FPERC, the IAC, the DR&PW Management and Other Officials to carry out their responsibilities.

6.9 External Audit

The responsibilities of external audit with regard to risk management in the DR&PW are to:

a) Determine whether the DR&PW Risk Management Policy, Risk Management Strategy and Risk Management Implementation Plan are in place and are appropriate.
b) Assess the effectiveness and efficiency of the implementation of the DR&PW Risk Management Policy, Risk Management Strategy and Risk Management Implementation Plan.
c) Review the risk identification process to determine if it is sufficiently robust to facilitate the timely, correct and complete identification of significant risks, including new and emerging risks.
d) Review the departmental Risk Assessment Process to determine if it is sufficiently robust to facilitate timely and accurate risk rating and prioritization.
e) Determine whether the DR&PW Management Action Plans to mitigate the key risks are appropriate, and are being effectively and efficiently implemented.

6.10 The Northern Cape Provincial Treasury (NCPT)

The responsibilities of the NCPT with regard to risk management in the DR&PW are to:

a) Prescribe uniform norms and standards.
b) Monitor and assess the implementation of the Public Finance Management Act (PFMA), 1999, as amended.
c) Assist the Department in building its capacity for efficient, effective and transparent financial management.
d) Enforce the PFMA.
e) Monitor and assess, amongst other things, the implementation of risk management in the DR&PW, including any prescribed norms and standards, including those from the National Treasury.
f) Assist the Department in building its capacity for, amongst other things, efficient, effective and transparent management, and particularly risk management.
g) Enforce the legislation and any other relevant risk management norms and standards as it applies to the DR&PW.

6.11 The DR&PW Internal Audit Committee (IAC)

6.11.1 The overall responsibilities of the departmental IAC with regard to risk management are to:

a) Review and recommend disclosures on matters of risk in the Department's annual financial statements.

b) Review and recommend disclosures on matters of risk and risk management in the DR&PW Annual Report.

c) Provide regular feedback to the AO on the adequacy, effectiveness and efficiency of risk management in the DR&PW, including recommendations for improvement, inclusive of the assessments and recommendations of the FPERC, which is a sub-committee of the IAC.

d) Ensure that the Internal and External Audit Plans are aligned to the Risk Profile of the Department.

e) Satisfy itself that it has appropriately addressed the Financial Reporting Risk, the risk of fraud and/or corruption, Internal Financial Controls and ICT risks as they relate to financial reporting in the Department.

f) Evaluate the effectiveness of the Internal Audit function in its responsibilities regarding risk management in the DR&PW.

6.11.2 The appointment of a properly constituted and qualified IAC will enable the Executing Authority, the AO and the Executive Management with a means to monitor an effective internal control system regarding risk management. In addition, the IAC reinforces both the internal control system and the internal audit function.

6.11.3 The approved risk management functions, authority and duties of the IAC must be defined and outlined in written format and included in the Terms of Reference of the IAC.

6.11.4 It must be disclosed in the Annual Report of the DR&PW whether or not the IAC has satisfied its risk management responsibilities for the financial year, in compliance of the above mentioned approved functions, authority and duties.

6.11.5 The IAC must furthermore review the following as it relates to risk management in the DR&PW:

a) The functioning of the internal control system.

b) The functioning of the Internal Audit and Risk Management section.

c) The functioning of the internal Financial Inspectorate section.

d) The risk areas of the DR&PW's operations to be covered in the scope of the external and internal audits.

e) The reliability and accuracy of the financial information provided to Management and other

users of financial information; and whether the DR&PW can rely on the accuracy of the current internal and external auditors.

f) Any accounting or auditing concerns identified as a result of the internal and external audits.

g) The DR&PW's compliance with legal and regulatory provisions, the departmental Code of Ethics and Conduct and the Code of Conduct of the Public Service at large, applicable municipal by-laws and the departmental policies, procedures, strategies and plans.

6.11.6 The IAC must, *inter alia*, also accomplish the following in terms of risk management in the DR&PW:

a) Promote proper communication between the Office of Political Oversight (MEC), members of the Executive Management, the Senior Management, the Internal Audit and Risk Management section, as well as the external auditor(s).

b) Confirm that the current Internal Audit Plan of the Department is in compliance with, and aligned to this policy and other relevant departmental policies, strategies and plans as they relate to risk management.

c) Develop a direct, strong and candid relationship with the external auditor(s).

d) Present the minutes of its meetings as it relates to risk management in the Department to the meetings of the Senior Management at least once every quarter or as requested by the AO.

e) Investigate any other related matters within its approved functions, authority and duties and safeguard all information supplied to it in accordance with the Minimum Information Security Standards (MISS) Policy of the South African Government, as approved by Cabinet.

7. DR&PW APPROACH TO RISK MANAGEMENT

7.1 The Department's Risk Management Terms of Reference, Code of Ethics and Conduct, as well as Ethics, Fraud and Corruption Management and Prevention Policies and Strategies will form an integral part of the DR&PW's Risk Management Implementation Plan.

7.2 The Department has developed and implemented basic internal control measures in its key operational areas.

7.3 The DR&PW is committed to maintain internal control measures, which are practical, effective and efficient.

8. PROCEDURES

The DR&PW will maintain procedures to provide for a systematic view of risks faced in the course of the Department's activities. This will require the Department to:

8.1 Establish Context and Objectives

Departmental risk management include the strategic, organisational and risk management context against which the risk management process in the DR&PW will take place. Criteria against which risks will be evaluated must be established and the structure of the risk analysis must be defined. The objectives of the DR&PW must also be taken into consideration and be defined properly.

8.2 Identify Risk

This refers to the identification of what, why and how events arise or may arise as the basis for further analysis, based on available evidence, which in turn forms the foundation for the development of forward-looking Risk Projections and the conception of Risk Scenarios.

8.3 Analyse and Evaluate Risk

This refers to the determination of existing controls and the analysis of risks in terms of consequences and likelihood in the context of those controls. The analysis must consider the range of potential consequences and how likely those consequences are to occur.

8.4 Treat Risk

For higher priority risks, the Department is required to develop and implement specific Risk Management Plans. Lower priority risks may be accepted and monitored.

8.5 Monitor and Review

This refers to the Risk Oversight and Review Management System and any changes that might affect it. Monitoring and reviewing occurs concurrently throughout the risk management process.

8.6 Communication and Consultation

Appropriate communication and consultation with internal and external stakeholders must occur at each stage of the risk management process as well as in the process as a whole. In this regard, it must be taken into account that the various stakeholders have their own subjective risk perceptions that will impact risk management in the Department.

8.7 Creating Awareness

For risk management to be successful, the Department will maintain an effective awareness campaign divided into two (2) categories namely:

a) Education; and

b) Communication.

The FPERC will provide continuous input into the DR&PW's Risk Management Policies and Strategy through reviews and evaluation. See Diagram 1 below regarding the process involved in risk management.

Diagram 1: The Risk Management Process

9. REPORTING ON RISK MITIGATION

9.1 Senior Managers are Risk Owners and will be required to report regularly on progress relating to mitigation of risks related to their Directorates/Chief Directorates.

9.2 The reporting format designed by the CRO and approved by the HOD include risks identified by the Risk Owners, which will be used for the purpose of regular reporting to the Sub-directorate Internal Inspectorate, in order to ensure that Risk Mitigation Action Plans are implemented.

9.3 The CRO will present a Risk Management Report to both the FPERC and the Senior Management, which will ultimately be signed-off by the HOD.

9.4 In considering and reviewing the reports on risk management and internal control in the course of a financial year, the Executive Management of the Department must:

a) consider what the DR&PW's risks are and how they have been identified;
b) assess the effectiveness of the related process of risk management, and particularly reports of significant failings or weaknesses in the process;
c) consider if the necessary action is being taken in a timely fashion to rectify any significant failings or weaknesses; and
d) consider whether the results obtained from the review process indicate that more extensive monitoring is required.

10. DEPARTMENTAL RISK TOLERANCE

The DR&PW must ensure the establishment of Risk Tolerance Rating Levels by Management.

11. ASSESSMENT OF RISK MANAGEMENT EFFECTIVENESS

11.1 Evaluation of risk management effectiveness is vital to maximise the value created through the risk management practices of the DR&PW.

11.2 The Department will strive to achieve a mature risk management regime in order to realise its risk management goals and objectives.

11.3 The Department will periodically evaluate its risks by measuring outcomes against preset key performance indicators.

11.4 See tables one (1) and two (2) below regarding Risk Likelihood and Risk Impact respectively, in terms of the Risk Rating Calculation Guidelines.

RISK LIKELIHOOD AND IMPACT RATING GUIDELINES:

Table 1: Risk Likelihood

Likelihood Rating		
Score	***Assessment***	***Definition***
1	*Rare*	The risk is conceivable but it's likely to occur only in extreme circumstances.
2	*Unlikely*	The risk occurs infrequently and is likely to occur within the next three (3) years.
3	*Moderate*	There is an above average chance that the risk will occur at least once in three (3) years.
4	*Likely*	The risk could easily occur and is likely to occur at least once within the next twelve (12) months.
5	*Common*	The risk is already occurring, or is likely to occur more than once within the next twelve (12) months.

Table 2: Risk Impact

Impact Rating		
Score	***Impact***	***Definition***
1	*Insignificant*	Negative outcomes or missed opportunities that are likely to have a negligible impact to meet objectives.
2	*Minor*	Negative outcomes or missed opportunities that are likely to have a relatively low impact to meet objectives.
3	*Moderate*	Negative outcomes or missed opportunities that are likely to have a relatively moderate impact to meet objectives.
4	*Major*	Negative outcomes or missed opportunities that are likely to have a relatively substantial impact to meet.
5	*Critical*	Negative outcomes or missed opportunities that are of critical importance to the achievement of the objectives.

11.4 Assessment Results

A risk is allocated a risk rating based on the assessment of its impact and likelihood. The risk rating of a risk is defined as the product of its assessment scores for impact and likelihood.

Formula: **Likelihood score X Impact score = Risk rating.**

CONSOLIDATED RISK RATING GUIDELINES (Likelihood X Impact):

Table 3: Risk Rating

Consolidated Risk Rating		
Risk rating	***Risk Priority***	***Action***
15 to 25	*High*	Take immediate action to reduce risk to acceptable.
8 to 14	*Medium*	Closely monitor risk and take action if necessary.
1 to 7	*Low*	Take no action-monitor periodically.

12. MONITORING AND EVALUATION (M&E)

12.1 The Directorate Internal Audit and Risk Management, supported by the departmental Monitoring and Evaluation (M&E) Unit shall, on behalf of the HOD/AO, ensure amongst others, the following:

a) Efficient and effective implementation of this policy.
b) The accessibility of this policy to the intended stakeholders.
c) The implementation of measures to limit the possible abuse of this policy.
d) Submission of the required Monitoring and Evaluation (M&E) Reports related to the implementation of this policy.
e) Development of the necessary tools and processes to assess the outcome of the policy implications by all the stakeholders.

13. POLICY REVIEW AND AMENDMENT

13.1 This policy is effective from date of signature.

13.2 The assessment to determine the effectiveness and appropriateness of this policy will be done five (5) years after its effective date. The assessment could be performed earlier than five (5)

years to accommodate any substantial structural or other organizational changes at the DR&PW or any change required by law.

13.3 If and when any provision of this policy is amended, the amended provision will supersede the previous one.

13.4 Deviations from this policy must be approved by the Accounting Officer (AO) of the DR&PW.

14. VIOLATION AND ENFORCEMENT

14.1 Any failure to comply with this policy will be viewed as a serious disciplinary transgression and could lead to disciplinary action taken against the offending employee(s) in terms of the Public Service Regulations and Code of Conduct, the DR&PW Code of Ethics and Conduct, as well as the other applicable policies in the DR&PW Compilation of Policies on Fraud, Corruption and Ethics Management, 2020, called *The Plan.*

14.2 Any employee that contravenes the provisions of this policy shall be charged with misconduct and/or fraud and corruption and will be held liable for any damages suffered by the state as a result of non-compliance.

14.2 Furthermore, those employees found to have connived or committed irregularities, including fraud and/or corruption and related matters, may be summarily dismissed from the public service.

14.4 Individuals who have been found guilty of violating this policy shall be prohibited from conducting any future business with the state; and, depending on the severity of the offence, legal action may be taken against the perpetrator(s); and if it is discovered that fraud and/or corruption was involved, the case will be reported to the SAPS for investigation and prosecution.

15. APPROVAL OF THE POLICY AND DATE OF EFFECT

This policy is Approved / ~~Not Approved~~

Comments:

.....

.....

.....

.....

.....

DR. J. MAC KAY
ACCOUNTING OFFICER

20.03.2023
DATE