NORTHERN CAPE

OFFICE OF THE PREMIER

RISK MANAGEMENT POLICY

2015/16

DOCUMENT CONTROL

Document Details	
Province	Northern Cape
Document	Risk Management Policy
Document Name	NCOTP_Risk_Management_Policy_V1_201516.doc
Document Number:	Version 1
Document Status:	Draft
Customer Contact	
Customer Reference:	
File Location:	
Author(s):	

Revision information		
Revision Number	**Revision Date**	**Change Reference**
1.0	1 February 2016	Initial Document

Document Approval				
Name	**Designation**	**Signature**	**Date**	**Approval (Y/N)**
Mr J. Bekebeke	**Director General**			

1. Contents

2. Background

The National Treasury recognises that risk management is a corporate and individual responsibility. The establishment of effective systems of risk management is a part of the framework of internal control. Anticipation of risks and subsequent management increases the enterprise's ability to respond to risks in a proactive manner, i.e. in a timely and appropriate manner.

To that end, management is responsible for ensuring that all risks, both internal and external, faced by the department are effectively managed. The approach utilised by management should provide a mechanism to formalise responsibility and establish accountability for all risk management activities, based on the consolidated risk report, in accordance with good governance.

The formalisation of risk management activities is often achieved through the establishment of a Risk Committee, which should compile the risk management plan.

The primary framework for developing the risk management plan should include:

- The establishment and maintenance of a common understanding of the risk universe that needs to be addressed in order to achieve the public department's objectives.
- Identification and agreeing the risk profile of the department.
- Co-ordinating the department's risk management and assurance efforts – to avoid duplication, ensure adequate coverage of the risks and decide on what assurance efforts are appropriate to provide the coverage.
- Considering the results/reports of the combined assurance efforts and to ensure that appropriate action is taken to address identified areas for improvement.
- Reporting to the Audit Committee on the work undertaken and extent of action taken by management to address identified areas for improvement. This reporting includes the Risk Committee's work in establishing and maintaining the understanding of the risks that need to be managed.
- Ensuring that the requirements of good governance are met.
- Identify and assess internal risks and opportunities attached to the different activities and resources of the public entities.
- Identify and evaluate new risks and opportunities arising from new objectives and external factors.
- Quantify potential liabilities and opportunities.
- Review past risks.

- Attempt to anticipate future risks and changes by monitoring internal and external environments to obtain information that may signal a need to re-evaluate the entity's objectives or control.

Once risks and opportunities have been identified and the likelihood and consequences of their occurring have been evaluated, appropriate policies and procedures can be established to manage them, proportionate to the risk or opportunity involved.

Risks not previously identified or those that may only emerge as circumstances change should be responded to in terms of the risk management philosophies developed i.e.:

- Prioritise.
- Assess effectiveness of current response.
- Identify any action needed to address the risk; and
- Develop a combined assurance approach for the risk (if appropriate)

Additional initiatives to strengthen and more effectively provide for risk management in the department include:

- Fully integrating risk identification, assessment and management with business and project planning at all levels, as well as in individual performance contracts and assessments; and
- Reviewing risk management policy, procedures and application within the relevant department's individual business groups or subsidiary companies.

The risk management plan should also clearly identify the role players in the risk assurance processes, for example: The role of internal audit is to actively monitor the internal and external environment and, if identified risks are not responded to appropriately, to be the catalyst for ensuring that the risk universe is continually updated.

An essential focus of King III is that the Board should "exercise leadership to prevent RISK MANAGEMENT from becoming a series of activities that are detached from the realities of the Company business". Risk is positioned, as a cornerstone of corporate governance and RISK GOVERNANCE is substantially different to the requirement to implement RISK MANAGEMENT. Greater emphasis is placed on the Board to ensure that it is satisfied with the MANAGEMENT OF RISK (delegated to the Audit

Committee in terms of Treasury Chapter 2 hand-out that talks to the Responsibilities of the Audit Committees).

3. Introduction

The Accounting Officer has committed Office of the Premier to a process of risk management that is aligned to the principles of good corporate governance, as supported by the Public Finance Management Act (PFMA), Act 1 of 1999 as amended by Act 29 of 1999.

The Information Communication Technology ICT Risk Management Policy is a component of a wider Enterprise Risk Management Policy associated with the use, ownership, operation, involvement, influence and the adoption of ICT.

4. Risk and Risk Management

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 Management must be aware of and be prepared to exploit. Such opportunities are encompassed in this definition of risk.

Risk management is a systematic and formalised process instituted by the department to identify, assess, manage and monitor risks.

4.1 Benefits of Risk Management

The Office of the Premier implements and maintains effective, efficient and transparent systems of risk management and internal control. The risk management will assist the department to achieve, among other things, the following outcomes needed to underpin and enhance performance:

- more sustainable and reliable delivery of services;
- informed decisions underpinned by appropriate rigour and analysis;
- innovation;
- reduced waste;
- prevention of fraud and corruption;
- better value for money through more efficient use of resources; and
- better outputs and outcomes through improved project and programme management.

5. Purpose of the Policy

The purpose of this Policy is to articulate the Office of the Premier's risk management philosophy. The Office of the Premier recognizes that risk management is a systematic and formalized process to identify, assess, manage and monitor risks and therefore adopts a comprehensive approach to the management of risk. Furthermore, the Policy seeks to to integrate risk management within the ICT framework to be implemented and maintained by the Office of the Premier.

6. Scope of the Policy

The scope is extended to those stakeholders and its service providers. This policy applies throughout the department within as far as risk management is concerned. The Policy also ensures the physical security to protect the state's information technology assets and vital business functions of all information resources whether managed internally or hosted externally. All stakeholders are expected to operate within the permissible parameters and implement Risk management Programs including the remediation of the identified risks in a timely manner.

- This policy must be read in conjunction with the following documents:
  I. Corporate Governance of ICT Policy
  II. Password Policy
  III. Acceptable Use Policy
  IV. Information Security Policy [Does not Make sense]

7. The Policy

The realization of our strategic plan depends on us being able to take calculated risks in a way that does not jeopardize the direct interests of stakeholders. Sound management of risk will enable us to anticipate and respond to changes in our service delivery environment, as well as take informed decisions under conditions of uncertainty.

We subscribe to the fundamental principles that all resources will be applied economically to ensure:

- The highest standards of service delivery;

- A management system containing the appropriate elements aimed at minimising risks and costs in the interest of all stakeholders;
- Education and training of all our staff to ensure continuous improvement in knowledge, skills and capabilities which facilitate consistent conformance to the stakeholders expectations; and
- Maintaining an environment, which promotes the right attitude and sensitivity towards internal and external stakeholder satisfaction.

An entity-wide approach to risk management is adopted by the office of the Premier, which means that every key risk in each part of the department will be included in a structured and systematic process of risk management. It is expected that the risk management processes will become embedded into the department's systems and processes, ensuring that our responses to risks remain current and dynamic. All risk management efforts will be focused on supporting the departmental objectives. Equally, they must ensure compliance with relevant legislation, and fulfill the expectations of employees, communities and other stakeholders in terms of corporate governance.

8. Legislative Mandates

1. Public Finance Management Act
2. Treasury Regulations
3. Public Sector Risk Management Framework
4. Northern Cape Provincial Information Security Policy, Version 1.2 of 2014;
5. Public Service Act, 1994;
6. Public Service Regulations, 2001;
7. State Information Technology Agency Act 88 of 1998;
8. Minimum Information Security Standards (MISS) approved in 1996.
9. National Intelligence Agency Act 39 of 1994;

9. Information Technology

Information Management primary role is the proper management of the ICT infrastructure. In the process, all risk related to ICT should be mitigated and controlled. The Policy seeks to address the elements of Risk Management within the ICT framework to be implemented and maintained, which will allow for the management of risk within the defined risk, risk appetite and tolerances as well as risk management standards as defined in this Policy.

The Policy covers all information resources whether managed internally or hosted externally. All stakeholders are expected to operate within the permissible parameters and implement Risk management Programs including the remediation of the identified risks in a timely manner.

The Policy further seeks to:

- Integrate risk management practices across the entity's ICT;
- Foster an environment where staff assumes responsibility for managing risks.
- Ensure that employees are aware that the use of appropriate risk management procedures.
- Appropriate risk management processes must be adopted for all phases of the information system lifecycle.
- Adoption of a risk management plan in the approval, review and control of all ICT related projects.
- ICT risk management will be transparent and include appropriate and timely involvement of stakeholders and decision makers.
- This policy applies to all personnel (Including contractors, interns and volunteers.)
- The Policy applies to all external organizations and their personnel who have been granted access to Information and Communications Technology (ICT) infrastructure and services.

10. POLICY DETAILS

Office of the Premier, will implement an appropriate Information Technology (IT) Risk Management Program to ensure the timely delivery of critical automated business services to their clients, stakeholders and citizens. This Program include the identification, classification, prioritisation and mitigation processes necessary to sustain the operational continuity of mission critical information technology systems and resources.

10.1 RISK MANAGEMENT FRAMEWORK

The framework assists in managing ICT risks effectively through the application of the risk management process at varying levels and within the ICT contexts.

10.1.1 Establish the Context:

Evaluating the entity's external context shall include, but is not limited to:

- The legal, financial, technological, natural and competitive environment, whether international, national, regional or local;
- Key drivers and trends having impact on the entity's ICT objectives; and relationships with, and perceptions and values of, external stakeholders in as far as they have bearing on ICT systems

Evaluating the entity's ***internal context*** shall include, but is not limited to:

- ICT governance, organizational structure, roles and accountabilities;
- ICT policies, objectives, and the strategies that are in place to achieve them;
- Capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- Actual information systems, information flows and decision making processes (both formal and informal);
- The organization's culture;
- ICT standards, guidelines and models adopted by the Office of the Premier;
- The form and extent of contractual relationships.

The management of ICT risk should be undertaken with full consideration of the need to justify the resources used in carrying out such risk management. The resources required, responsibilities and authorities, and the records is specified in the risk register.

10.1.2 Risk Identification:

Identification of the entity's ICT risks shall include, but is not limited to the following categories:

- Information Security Risk;
- Facilities and Environmental Controls Risk;
- Change Control Risk;
- Firewall Risk;
- Internet Connection Risk;
- Password Risk;
- Patch Management Risk;
- User Access Risk;
- Vulnerability Management Risk;

- Disaster Recovery Risk.

10.1.3 Risk Analysis

ICT risk analysis may be undertaken with varying degrees of detail, depending on the risk, the purpose of the analysis, and the information, data and resources available. Analysis can be qualitative, semi-quantitative or quantitative, or a combination of these, depending on the circumstances.

10.1.4 Risk Evaluation

The ICT risk evaluation process should assist in making decisions, based on the outcomes of analysis, about which risks need treatment and the priority for treatment implementation as per Risk Register.

10.1.5 Risk Treatment

Risk Treatment is the process of selecting and implementing of measures to modify risk. Risk treatment measures can include avoiding, optimizing, transferring or retaining risk.

The Risk Management process that is applied at a departmental level to manage and mitigate risks is through the utilization of a Risk Register framework as a tool for Risk Treatment.

- The Risk Register documents the identification, analysis, and assessment of risks and summarizes existing and proposed risk controls and measures.

The format of the Risk Register will be progressively refined within the department to ensure a brief and efficient process that fits within current quality assurances.

10.1.6 Implementing a Risk Management Plan

Risk Management Plan is implemented on a quarterly basis and as a need arises using the IT risk register

10.1.7 Risk Monitoring and review.

Risk Monitoring and review is done on a quarterly basis and as a need arises using the IT risk register

10.1.8 Risk Management Program activities

The Office of the Premier's Risk Management programs should focus on the following four types of activities:

	Activity	Action
1	**Identification of Risks**	A continuous effort to identify which risks are likely to affect business continuity and security functions and documenting their characteristics.
2	**Analysis of Risks**	An estimation of the probability, impact, and timeframe of the risks, classification into sets of related risks, and prioritisation of risks relative to each other.
3	**Mitigation Planning**	Decisions and actions that will reduce the impact of risks, limit the probability of their occurrence, or improve the response to a risk occurrence. For important risks, mitigation plans should be developed.
4	**Tracking and Controlling Risks**	Collecting and reporting status information about risks and their mitigation plans, responding to changes in risks over time, and taking corrective actions as needed.

11. Role players

Every employee is responsible for executing risk management processes and adhering to risk management procedures laid down by the department management in their areas of responsibilities.

11.1 Risk Management Oversight

11.1.1 Executive Authority

The Executive Authority takes an interest in risk management to the extent necessary to obtain comfort that properly established and functioning systems of risk management are in place to protect the department against significant risks.

11.1.2 Audit Committee

The Audit Committee is an independent committee responsible for oversight of the department's control, governance and risk management. The responsibilities of the Audit Committee with regard to risk management are formally defined in its

charter. The Audit Committee provides an independent and objective view of the department's risk management effectiveness.

11.1.3 Risk Management Committee

The Risk Management Committee is appointed by the Accounting Officer to assist them to discharge their responsibilities for risk management. The Committee's role is to review the risk management progress and maturity of the department, the effectiveness of risk management activities, the key risks facing the department, and the responses to address these key risks. The responsibilities of the Risk Management Committee are formally defined in its charter.

11.2 Risk Management Implementers

11.2.1 Accounting Officer

The Accounting Officer is the ultimate Chief Risk Officer of the department and is accountable for the department's overall governance of risk. By setting the tone at the top, the Accounting Officer promotes accountability, integrity and other factors that will create a positive control environment.

11.2.2 Management

Management is responsible for executing their responsibilities outlined in the risk management strategy and for integrating risk management into the operational routines.

11.2.3 Other Officials

Other officials are responsible for integrating risk management into their day-to-day activities. They must ensure that their delegated risk management responsibilities are executed and continuously report on progress.

Training will be provided for all organizational staff and volunteers so they understand the rationale of the risk management plan as well as the expectations, procedures, forms,

11.3 Risk Management Support

11.3.1 Chief Risk Officer

The Chief Risk Officer is the custodian of the Risk Management Strategy, and coordinator of risk management activities throughout the department. The primary responsibility of the Chief Risk Officer is to bring to bear his/her specialist expertise to assist the department to embed risk management and leverage its benefits to enhance performance.

11.3.2 Risk Champion

The Risk Champion's responsibility involves intervening in instances where the risk management efforts are being hampered, for example, by the lack of co-operation by Management and other officials and the lack of departmental skills and expertise.

11.4 Risk Management Assurance Providers

11.4.1 Internal Audit

The role of the Internal Auditing in risk management is to provide an independent, objective assurance on the effectiveness of the department's system of risk management. Internal Auditing must evaluate the effectiveness of the entire system of risk management and provide recommendations for improvement where necessary.

11.4.2 External Audit

The external auditor (Auditor-General) provides an independent opinion on the effectiveness of risk management.

An entity-wide approach to risk management will be adopted by the Institution, which means that every key risk in each part of the Institution will be included in a structured and systematic process of risk management. It is expected that the risk management processes will become embedded into the Institution's systems and processes, ensuring that our responses to risk remain current and dynamic. All risk management efforts will be focused on supporting the Institution's objectives. Equally, they must ensure compliance with relevant legislation, and fulfill the expectations of employees, communities and other stakeholders in terms of corporate governance.

12. Policy review

This Policy shall be reviewed annually to reflect the current stance on risk management.

The Policy is endorsed by Risk Management Committee and approved by the Accounting Officer.