



LIMPOPO

PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF SOCIAL DEVELOPMENT

Risk Management **Policy**

TABLE OF CONTENTS

PAGES

1. Policy Statement	3
2. Introduction	3
3. Legal mandates	4
4. Purpose of the policy	4-5
5. Policy objectives	5
6. Scope of the policy	5-6
7. Definition of concepts	6
8. Risk Management approach	7
8.1 Risk identification	7-8
8.2 Risk evaluation	8-11
8.3 Risk control	11-13
8.4 Risk financing	13-15
8.5 Risk monitoring	15
9. Internal and external Stakeholders in managing risk	15
9.1 Executive Authority	16
9.2 Accounting officer	16
9.3 Risk Management Committee	17-18
9.4 Chief Risk Officer	18
9.5 Management	19
9.6 Other officials	19
9.7 Internal Audit	19
9.8 External Audit	20
9.9 Audit Committee	20
9.10 Provincial Treasury	20
10. Policy review	20

- The highest standards of service delivery;
- A management system containing the appropriate elements aimed at minimizing risks and costs in the interest of all stakeholders;
- Education and training of all staff to ensure continuous improvement in knowledge, skills and capabilities; and
- Maintaining an environment which promotes the right attitude and sensitivity towards internal and external stakeholder satisfaction.

3. Legal mandates

The policy is informed by the following prescripts:

- 3.1 The Constitution of RSA, 1996, as amended.
- 3.2 The Public Finance Management Act, 1999 (Act 1 of 1999), as amended.
- 3.3 Treasury Regulations 2002 (issued in terms of PFMA)
- 3.4 The Public Service Act (1999), as amended.
- 3.5 Public Service Regulations, 2001.
- 3.6 Public Sector Risk Management Framework, 1 April 2010.
- 3.7 The Prevention and Combating of Corrupt Activities Act, 2004 (Act 12 of 2004)
- 3.8 The Protected Disclosure Act, 2000 (Act 20 of 2000)
- 3.9 Promotion of Access to Information Act, 2000 (Act no 2 of 2000).
- 3.10 Promotion of Administrative Justice Act, 2000 (Act 3 of 2000)
- 3.11 The Labour Relations Act, 1995 (Act 66 of 1995)
- 3.12 National Archives and Records Services Act, 1996 (Act 43 of 1996)
- 3.13 Occupational Health and Safety Act, 1993 (Act 85 of 1993).
- 3.14 Disaster Management Act 57, 2002 (Act 57 of 2002)
- 3.15 The Minimum Information Security Standards, 4 December 1996.
- 3.16 King III Code of Good Corporate Governance for South Africa 2009.

A

	systems failure leading either to error or loss of business, non-development of systems and implementation failures, Insufficient systems capacity, poor data integrity, security breaches.
People	The risks arising from the possibility of incompetent, inexperienced and/or negligent staff, unauthorized activity, the risk of human error with specific regard to processing, the risk that a working culture may lead to low morale; high turnover of staff; low productivity and industrial action, the risk of fraudulent and other criminal activity, lack of segregation of duties, lack of integrity and honesty, lack of control, the risk associated with ill informed decision.
External	Risks arising from natural disasters, external criminal activities, industrial and labor unions strikes, risks associated with third parties, for examples, suppliers and contractors. Deterioration of the department's reputation as perceived by the clients.

7. Definition of concepts.

- 7.1 **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).
- 7.2 **Risk management** is a systematic and formalized process instituted by the department to identify, evaluate, manage and monitor risks.
- 7.3 **Enterprise Risk Management (ERM)** is a coordinated approach to assessing and responding to all risks that affect the achievement of an organization's strategic and financial objectives.
- 7.4 **Strategic risk** refers to a wide range of possible events and scenarios which can impact on business's strategy execution, including the ultimate impact on the valuation of an organization.
- 7.5 **Operational risk** is the exposure of an organization to potential losses, resulting from shortcomings and/or failures on the execution of its operations. These losses may be caused by internal failures or shortcomings of people, processes and systems, as well as the inability of people, processes and systems to cope with the adverse effects of external factors.
- 7.6 **Risk tolerance** is the amount of risk the department is capable of bearing as part of normal management practice. This level of acceptable risk establishes the benchmark for the department's risk tolerance.
- 7.7 **Management** means all members of the Senior and Middle Management Services, as well other Line Managers, except for the Accounting Authority, Chief Risk officer, other officials and officials reporting to the Chief Risk officer.
- 7.8 **Other Official** means an official other than the Accounting Authority, Management, Chief risk officer and his/her staff.

- iv) During the workshop identify the inherent risk for the business, as well as the measures required to eliminate or reduce the potential effect of the risk.

8.2. Risk evaluation.

There is a close and integrated link between risk identification and risk evaluation. The result of the risk identification process should be analyzed to serve as input for risk evaluation process. The evaluation of risk can be qualitative or quantitative in nature. The aim of risk evaluation is also to determine the potential impact of a loss event and the likelihood of a risk event occurring. This will provide management with guidelines on what control measures are required to prevent the event from occurring.

8.2.1 Risk analysis

After the risk has been identified, it is important that the inherent risk and the current control measures are analyzed. This can be regarded as a step connected with the risk evaluation process, and involves the rating of controls against the identified inherent risk. The objectives of risk analysis are to separate the minor acceptable risks from the major risks, and to provide data to assist in the evaluation and the treatment of the risks.

The results of the identification process, namely the inherent risks and controls, form the input for the risk analysis, while the rating of the inherent risks and controls, which identifies the major risks, forms the output of the initial analysis of the risk. The initially rated inherent risks and controls subsequently form the input for the first step of the risk evaluation process.

This step entails the analysis of risk exposures and the information gathered in the first step, as well as further analysis of the inherent risk identified in the risk identification process. This analysis can be achieved by means of an assessment framework as illustrated in table 1.3. In addition, the framework also aims to evaluate the control measures in order to determine the residual risk

Table 3: Risk assessment framework

Risk	Inherent Risk		Inherent Risk Exposure Index	Current control	Control Effectiveness	Residual Risk Exposure	Mitigation measure	Risk owner	Cost of mitigation	Time Frame
	Impact	Likelihood								

A

Insignificant	Negative outcomes or missed opportunities that are likely to have a relatively negligible impact on the ability to meet objectives	1
----------------------	--	---

8.2.3.2 Likelihood

The likelihood that a risk might occur should be assessed by taking into account the current conditions and the process available to restrict the chance of the event occurring. The assessment of the likelihood or frequency of a risk event occurring can be determined in terms of the following:

Table 5: Scale to determine the likelihood of risk occurrences.

Likelihood category	Category definition	Factor
Common	The risk is already occurring, or is likely to occur more than once within the next 12 months.	5
Likely	The risk could easily occur, and is likely to occur at least once within the next 12 months	4
Moderate	There is an above average chance that the risk will occur at least once in the next three years	3
Unlikely	The risk occurs infrequently and is unlikely to occur within the next three years	2
Rare	The risk is conceivable but is only likely to occur in extreme circumstances	1

8.2.3.3. Existing Controls

Participants should assess the existing control effectiveness based on their understanding of the control environment currently in place in the department. This is a measure of how well management perceives the control process to be working effectively managing the risk. The identified controls can be rated according to the following rating scale

the department. The controls should minimize the loss when it occurs and when preventative methods have not been fully effective. Risk control can thus be seen as an activity for the mitigation of risk. This component of risk management process can include activities such as the implementation of the policies and procedures, internal controls, risk reporting and decision making, as well as the organizational structure to form the basis of the process.

It is imperative that after the controls have been formulated, management ensures that they are aligned with the original business objectives.

8.3.1 The concept risk control

Risk control entails any activity that is aimed at the prevention of losses, the minimization of the consequences of losses that may arise from any risks facing the department, and the handling of an adverse event in advance or as it occurs. It is essential for an organization to have the following three types of risk control in place in order to mitigate operational risk.

- i) **Preventative controls.** These are control measures that are put in place in order to prevent a loss event from occurring, for example, segregation of duties in order to prevent fraud and errors of employees.
- ii) **Detective controls.** These are control measures that ensure that a loss is identified as soon as it occurs, in order to control the effect on the department and to put preventative controls in place to prevent re-occurrence.
- iii) **Contingency controls.** These control measures are necessary in order to ensure the sustainability of the department once a risk event has occurred, for example, a backup site that is available if a computer Centre is flooded.

It is important that the risks underlying risk factors be distinguished in order to match the relevant mitigating controls. see examples on table 1.7 below:

Table 8: Operational risks mapped to mitigating controls

Risk	Mitigating systems and controls
Child neglect by foster parents.	Awareness education, e.g conduct parenting skills workshop to foster parents and also develop a prospective Foster parents register.
Loss of information.	Develop a Disaster recovery plan
Slow response of IT systems.	Increase the bandwidth on the critical sites.
Projects failing to account on funded	Motivate for the incorporation of monitoring NPO funding as KRA for Finance personnel and capacitate both Social workers and NPOs

A

the department. Hence, the cost of risk should reflect the cost efficiency and ensure optimal financing.

8.4.1 The cost of risk

The cost of risk can be the sum total of the following:

- i) Internal controls and loss prevention expenses, for example, the cost of segregation of duties, the cost of hardware and software for the elimination of manual intervention and human errors.
- ii) The cost of external evaluation programs that determine the effectiveness of the processes and procedures, for example, the cost of procedure manuals, the cost of training of supervisors who implement the control measures.
- iii) Unreimbursed and unrecovered operational losses.
 - There are always losses that the department writes off in the financial statement as irrecoverable losses, e.g. Of events such as internal and external frauds, system failures, negligence and errors, processing problems. Sometimes recovery of such events is possible by means of credit control, legal actions or repossessions, however, most of the time the department will incur a certain irrecoverable loss.
- iv) External insurance premiums
 - These insurance premiums refer to third party insurance. In such cases, the potential effect of a possible loss is event is shared with a third party (insurer) at a preset cost to the department. it is important for risk managers to understand the various costs involved in financing operational risk in order to ensure that the cost of risk is realistic in comparison to the potential rewards and benefits that the department can derive from the management of risks.
- v) Maintenance and management costs, for example staff costs of risk practitioners, external consultancy services)

8.4.2 Risk financing program

The department has the following two fundamental options with regard to risk financing:

- i) The retention of the risk. In such instances the department decides that the risk may be tolerated. The department monitors the exposures in order to ensure that the risk does not become financially intolerable. The department may also adopt a self-insurance mechanism whereby it allocates its own funds to cover potential losses. After determining the total residual risk exposure of the department by means qualitative and quantitative methods, the management can determine the risk tolerance of the department. The risk tolerance is the financial amount which the department is prepared to accept and tolerate as a

9.1 Executive Authority

The Executive Authority shall take 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.

The Executive Authority is accountable to the legislature in terms of the achievement of the goals and objectives of the department. In this context the Executive Authority shall take 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.

9.2 Accounting Officer

The responsibility of the Accounting Officer is prescribed in terms of section 38 of the PFMA which stipulates that, *'The Accounting Officer for a department, trading entity or constitutional institution must ensure that the department, trading entity, or constitutional institution has and maintains effective, efficient and transparent systems of financial, risk management and internal controls.'*

The Accounting Officer is the ultimate Chief Risk Officer of the department and shall be accountable for the department's overall governance of risk. Accounting Officer shall promote accountability, integrity and other factors that will create a positive control environment.

Responsibilities of the Accounting Officer / Authority shall be as follows:

- a) Setting an appropriate tone by supporting and being seen to be supporting the Institution's aspirations for effective management of risks;
- b) Delegating responsibilities for risk management to Management and internal formations such as the Risk Management Committee.
- c) Holding Management accountable for designing, implementing, and monitoring and integrating risk management into their day-to-day activities;
- d) Providing leadership and guidance to enable Management and internal structures responsible for various aspects of risk management to properly perform their functions;
- e) Approving the risk management policy, strategy, and implementation plan;
- f) Approving the Institution's risk tolerance;
- g) Devoting personal attention to overseeing management of the significant risks;
- h) Leveraging the Audit Committee, Internal Audit, External Audit and Risk Management Committee for assurance on the effectiveness of risk management;
- i) Ensuring appropriate action in respect of the recommendations of the Audit Committee, Internal Audit, External Audit and Risk Management Committee to improve risk management; and
- j) Providing assurance to relevant stakeholders that key risks are properly identified, assessed and mitigated.

- (xi) Set out the nature, role, responsibility and authority of the risk management function within the Institution for approval by the Accounting Officer, and oversee the performance of the risk management function;
- (xii) Provide proper and timely reports to the Accounting Officer on the state of risk management, together with aspects requiring improvement accompanied by the Committee's recommendations to address such issues.

9.3.3 Meetings

The Committee shall meet at least four times per annum. The Chairperson of the Committee or a majority of the permanent members of the Committee may convene additional meetings as circumstances may dictate.

9.4. Chief Risk Officer (CRO)

The CRO is the Senior Official who is the head of the Risk Management Unit. He/she is the custodian of the Risk Management Strategy, and coordinator of risk management activities throughout the department. The primary responsibility of the CRO is to bring to bear his/her specialist expertise to assist the department to embed risk management and leverage its benefits to enhance performance.

The responsibilities of a CRO shall be to:

- a) Develop, in consultation with management, the department's risk management framework incorporating, *inter alia*, the risk management policy; risk management strategy; risk management implementation plan; risk identification and assessment methodology; risk tolerance; and risk classification.
- b) Communicate the department's risk management framework to all stakeholders in the department and monitoring its implementation;
- c) Facilitate orientation and training for the Risk Management Committee;
- d) Train all stakeholders in their risk management functions;
- e) Continuously drive risk management to acceptable National Treasury Standards;
- f) Assist Management with risk identification, assessment and development of response strategies;
- g) Monitor the implementation of the response strategies;
- h) Collating, aggregating, interpreting and analyzing the results of risk assessments to extract risk intelligence;
- i) Reporting risk intelligence to the Accounting Officer / Authority, Management and the Risk Management Committee; and
- j) Participating with Internal Audit, Management and Auditor-General in developing the combined assurance plan for the Institution.

9.8 External Audit

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

9.9 Audit Committee

The Audit Committee is an independent committee responsible for oversight of the department's control, governance and risk management. The Audit Committee shall provide an independent and objective view of the department's risk management effectiveness.


9.10 Provincial Treasury

The role of the Provincial Treasury in risk management shall be to provide an independent, objective assurance on the effectiveness of the department's system of risk management. Provincial Treasury must evaluate the effectiveness of the entire system of risk management and provide recommendations for improvement where necessary. Representatives from the Provincial Treasury shall be ex-officio members in the risk management committee.

10. Policy review

This Policy shall be reviewed after three (3) years and as and when a need arises.

Recommended~~not recommended~~

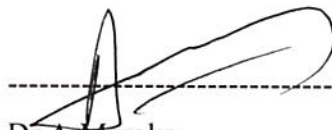


Ms Ramokgopa MD

Chairperson: Risk Management Committee

Date: 24/06/2011

Approved~~not approved~~



Dr A Morake

Head of the Department

Date:

27/7/11