

---

# **Mpumalanga Provincial Government of Education Department**

---



## **RISK MANAGEMENT STRATEGY 2014/2016**

---

## TABLE OF CONTENT PAGE NUMBER

<b>1. FOREWORD</b> .....	
1.1. POLICY OBJECTIVE .....	
1.2. POLICY STATEMENT.....	
1.3. LEGAL MANDATE.....	
<b>2. DEFINITION OF RISK MANAGEMENT</b> .....	
<b>3. RISK MANAGEMENT OBJECTIVES</b> .....	
<b>4. BENEFITS OF RISK MANAGEMENT</b> .....	
<b>5. RISK MANAGEMENT STRUCTURE AND RESPONSIBILITIES</b> .....	
5.1 EXECUTIVE AUTHORITY.....	
5.2 ACCOUNTING OFFICER.....	
5.3 MANAGEMENT.....	
5.4 AUDIT COMMITTEE.....	
5.5 RISK MANAGEMENT COMMITTEE.....	
5.6 CHIEF RISK OFFICER.....	
5.7 OTHER OFFICIALS.....	
5.8 INTERNAL AUDIT.....	
5.9 RISK CHAMPIONS.....	
<b>6. RISK MANAGEMENT PROCESS</b> .....	
<b>APPENDIX A: DEFINITIONS AND CRITERIA FOR WORK EVALUATION</b> .....	
1. DEFINITIONS.....	
2. CRITERIA FOR ASSESSING RISKS.....	
<b>APPENDIX B: RISK CATEGORY MODEL</b> .....	
7. REVIEW OF THE STRATEGY.....	
8. APPROVAL OF THE STRATEGY.....	

## 1. FOREWORD

The Accounting Officer for the Mpumalanga Department of Education has committed the Department 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 no. 1 of 1999 as amended by Act no. 29 of 1999*.

### 1.1. POLICY OBJECTIVES

The objective of this policy is to safeguard the government's property, interests, and certain interests of employees during the conduct of government operations.

### 1.2. POLICY STATEMENT

It is government policy to identify, and reduce or eliminate risks to its property, interests and employees, to minimize and contain the costs and consequences in the event of harmful or damaging incidents arising from those risks, and to provide for adequate and timely compensation, restoration and recovery.

### 1.3 LEGAL MANDATE

The Public Finance Management Act no.1 of 1999 supplemented by the relevant Treasury Regulations makes provision for best governance practices which have also been included in the revised King Report on Corporate Governance.

Section 38 (a) of the PFMA states that:

"The Accounting Officer...has and maintains:

- i) Effective, efficient and transparent systems of financial and risk management and internal control; and
- ii) A system of internal audit under the control and direction of an audit committee.....".

The extension of the general responsibilities, in terms of Section 45 of the PFMA, to all managers is a cornerstone in the institutionalisation of risk management in the public service. The extension also establishes accountability for risk management at all levels of management, and does not limit it to the Accounting Officer or Risk Management Unit.

The roles and responsibilities for the implementation of a Risk Management strategy are contained in the Treasury Regulations. Section 3.2 of the Regulations revolves around risk management and can be summarised as follows:

- a. The Accounting Officer must ensure that a risk assessment is conducted regularly to identify emerging risks for the institution.
- b. The Risk Management Strategy, which must include a fraud prevention plan, must be used to direct internal audit effort and priority and to determine the skills required of managers and staff to improve controls and to manage these risks.
- c. The strategy must be clearly communicated to all officials to ensure that the risk management strategy is incorporated into the language and culture of the institutions.

**1.4 King II Report on Corporate Governance reflects on risk management as an integral part of strategic and operational activities.**

- i. Risk Management is recognised as an integral part of responsible management and the Mpumalanga Department of Education is therefore adopting a comprehensive approach to the management of risks.
- ii. It is expected that all chief directorates, directorates, sections, operations and processes will be subject to the risk management strategy. It is the intention of the Department that all its sections work together in a consistent and integrated manner, with the overall objective of reducing risks.
- iii. Effective Risk Management is imperative to the Department to fulfil its mandate, the service delivery expectations of the public and the performance expectations within the Department.
- iv. The realisation of the Department strategic goals depends on the Department being able to take calculated risks in a way that does not jeopardise the direct interests of stakeholders. Sound management of risks 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.
- v. The Department subscribe to the fundamental principles that all resources will be applied economically to ensure:
  - a) The highest standards of service delivery
  - b) A management system containing appropriate elements that are aimed at minimising risks and cost in the interest of all stakeholders;
- vi. Education and training of all our staff to ensure continuous improvement in knowledge, skills and capabilities that facilitate consistent conformance to the stakeholders' expectations; and
- vii. Maintaining an environment that promotes the right attitude and sensitivity towards internal and external stakeholder satisfaction.
- viii. An entity-wide approach to risk management will be adopted by the Department, which means that every key risk in each part of the Department will be included in a structured and systematic process of risk management.
- ix. It is expected that risk management processes will become embedded into the Department's systems and processes, ensuring that responses to risks remain current and dynamic. All risk management efforts will be focused on supporting the Department's objectives.
- x. Equally, must ensure compliance with relevant legislations, and fulfil the expectations of employees, communities and other stakeholders in terms of corporate governance.

**1.5 The King III Report on Corporate Governance also reflects on risk management**

- i. The essential focus of the Code is that the Executive management should "exercise leadership to prevent risk management from becoming a series of activities that are detached from the realities of the Department's business."
- ii. In this context, risk is positioned as a cornerstone of corporate governance and risk governance is substantially different to the requirement to implement risk management.
- iii. Greater emphasis is placed on the executive management to ensure that it is satisfied with the management of risk.



## **1.6 Implication of King III report on Corporate Governance in the Department**

- i. The requirement is to disclose how the Executive Management has satisfied itself that risk assessments, responses and interventions are effectively evidenced.
- ii. Due care and diligence will need to be exercised and disclosed.

## **1.7 This due care and diligence is achieved through:**

- i. The structures of governance – Risk/Audit committee,
- ii. Adoption and implementation of an annual risk management plan,
- iii. Effective risk management practices through the application of recognised frameworks, methodologies, continuous assessments and monitoring,
- iv. Applying risk considerations into the decision making frameworks (at zero appetite and tolerance) and on specific decisions,
- v. Ensuring that the Executive Management receives adequate assurance on the effectiveness of the risk management process and on the management of specific risks;
- vi. Disclosing how the Executive Management is satisfied with the effectiveness of risk management.

## **2. DEFINITION OF RISK MANAGEMENT**

Risk management has been defined as *“a continuous, proactive and systematic process, effected by a Department’s executive authority, accounting officer, management and other personnel, applied in strategic planning and across the Department, designed to identify potential events that may affect the Department, and manage risks to be within its risk tolerance, to provide reasonable assurance regarding the achievement of Department objectives.”*

*(National Treasury, 2008f)*

## **3. RISK MANAGEMENT OBJECTIVES**

The Accounting Officer is responsible for ensuring that there is a sound system of risk management and control in place to:

- I. Safeguard the Department’s assets.
  - II. Support for the achievement of strategic objectives.
  - III. Behave responsibly towards all stakeholders.
  - IV. Ensure service delivery to all stakeholders.
- a. Effective risk management is therefore a key tool to ensure that the Department achieves its objectives. What is implicit in the above mentioned objectives is that:
1. Risk management does not just focus on managing downside risk. It is there to assist in identifying opportunities and to ensure that the risks involved in these opportunities are appropriately managed.
  2. The implementation of internal controls needs to carefully consider the benefits and costs i.e. the cost of control should not exceed the potential loss should the risk occur.
- b. A major component of risk management is the establishment of a risk register and fraud prevention plan. Managing the risk of fraud and corruption entails the

development, implementation, and maintenance of cost effective internal controls.

#### 4. BENEFITS OF RISK MANAGEMENT

The risk management process is being implemented by the Department as it will assist with the achievement of objectives. The benefits of risk management for the Department are:

- 4.1 Organisational alignment:** The risk management process is designed to complement effective strategic and operational planning. However, as the risk management approach is objective driven, it will assist in ensuring that management and employees understands and are committed to the key objectives which have been defined. This will include an understanding of the key performance indicators (KPIs) against which our success is measured.
- 4.2 Improved ability to manage risks:** By formally identifying and evaluating risks the Department will improve our understanding of the risks that have to be managed. Furthermore, we will analyse and understand the causes of risks to ensure our internal controls manage these causes.
- 4.3 Improved ability to achieve objectives:** By proactively identifying risks a Department will have a better understanding of risks and be more anticipatory and therefore able to achieve its objectives with greater certainty.
- 4.4 Improved ability to seize opportunities:** By understanding the risk profiles, the risk management process will enable the Department to seize and execute new opportunities successfully.
- 4.5 Cost Effective Internal Controls:** The risk management process will ensure that the system of internal control is cost effective. Areas of over control should be identified and removed.
- 4.6 Sustainability:** The risk management process is a means to educate all management and staff on their responsibility for risk management and the effective application of internal controls. Risk Management will be embedded at all levels within the Department.

Summarily, risk management helps the Department to achieve its objectives and prevents loss of resources, it ensures effective reporting and helps ensure that the Department complies with laws and regulations, avoiding damage to its reputation and other consequences. It also helps the Department to get to where it wants to go and avoid pitfalls and surprises along the way.

#### 5. RISK MANAGEMENT STRUCTURES AND RESPONSIBILITIES

##### 5.1 Member of Executive Authority (MEC)

The Executive Authority should take an interest in risk management to obtain comfort that properly established and functioning systems of risk management are in place to protect the Institution against significant risks.

The Executive Authority's responsibilities in risk management include the following:

- a) Ensuring that the Departmental strategies are aligned to the government mandate
- b) Obtain assurance from management that the Department strategies choices are based on a rigorous assessment of risks
- c) Assist the Accounting Officer to deal with fiscal, intergovernmental, political and other risks beyond his/her direct control and influence
- d) Insist on the achievement of objectives, effective performance management and value for money

## 5.2 Accounting Officer (HOD)

The Accounting Officer is ultimately responsible for and should assume “ownership” of risk management. More than any other individual, the Accounting Officer sets the “tone at the top” that affects integrity and ethics and other factors of the control environment.

In any Department, the Accounting Officer fulfils this duty by providing leadership and direction to Senior Managers and reviewing the way they manage the Department. The Accounting Officer is ultimately responsible for ensuring that a risk management process is implemented throughout the Department.

The Accounting Officer delegates responsibilities for risk management to management and internal structures (i.e.) Risk Management Committee, Fraud Prevention Committee, etc. The Accounting Officer holds management accountable for designing, implementing, monitoring and integrating risk management into their day-to-day activities; the Accounting Officer has a major role in defining what she/he expects in integrity and ethical values and can confirm expectations through oversight activities.

Similarly, by reserving authority in certain key decisions, the Accounting Officer plays a role in setting strategy, formulating high-level objectives and broad-based resource allocation.

The **Accounting Officer** provides oversight with regard to risk management by:

- a) Knowing the extent to which management has established effective risk management in the Department;
- b) Being aware of and concurring with the Department’s risk tolerance;
- c) Reviewing the Department’s portfolio view of risks and considering it against the Department’s risk tolerance; and
- d) Being aware of the most significant risks and whether management is responding appropriately.

## 5.3 Management

- a) Management is responsible for executing responsibilities outlined in the risk management strategy and for integrating risk management into operational routines.
- b) Management is accountable to the HOD for designing, implementing and



- monitoring the process of risk management and integrating it into the day-to-day activities of the Department.
- c) Management assigns responsibility for the establishment of more specific risk management policies and procedures to personnel responsible for individual units' functions.
  - d) A manager is effectively an accounting officer of his or her sphere of responsibility. Also significant are leaders of staff functions such as Compliance, Financial Management, Human Resources and Supply Chain Management, whose monitoring and control activities cut across, as well as up and down, the operating and other units of a Department.
  - e) Management is to maintain a co-operative relationship with the Risk Management Unit
  - f) Management is to present to the Risk Management and Audit Committee as requested
  - g) Management is to monitor the implementation of risk management within their area of responsibility and provide reports thereof.

#### **5.4 Audit Committee**

- a) The Audit Committee functions as a monitoring and oversight body to ensure that risk management is embedded in the Department.
- b) The responsibility of the Audit Committee with respect to risk management is formally defined in its charter.

#### **5.5 Risk Management Committee**

- a) The risk management committee is appointed by the Accounting Officer to assist the Department to discharge its responsibilities for risk management.
- b) The risk management committee is to comprise of senior management of the Department and the chairperson of the committee is an independent external person who is appointed by the Accounting Officer.
- c) The Risk Management Committee will assist the Accounting Officer in discharging its risk management responsibilities. The composition and Terms of Reference of this Committee is set out in a separate document, termed "Risk Management Committee Charter".

The Risk Management Committee is to review and recommend that the Accounting Officer approve the following:

- i. Risk management Policy
  - ii. Fraud Prevention Policy
  - iii. Risk management strategy
  - iv. Risk management implementation plan
  - v. Fraud Prevention strategy
  - vi. The Department's risk appetite
- d) The Committee evaluates the extent and effectiveness of integration of risk management within the Department
  - e) The committee assesses the implementation of the risk management policy and strategy
  - f) The committee interacts with the Audit Committee to share information relating to material risks of the Department
  - g) The Risk management committee provides timely and useful reports to the



Accounting Officer on the state of risk management, together with accompanying recommendation to address any deficiencies identified by the committee.

- h) Where there is a need for the Risk Management Committee to work through a sub-committee, it should obtain approval from the Accounting Officer for the establishment of such a sub-committee.
- i) The Risk Management Committee exercises control over the functioning of the sub-committee.

## **5.6 Chief Risk Officer (CRO)**

The primary responsibility of the CRO is to bring to bear specialist expertise to assist the Department to embed risk management and leverage its benefits to enhance performance.

The high level responsibilities of the CRO include:

- a) Developing, in consultation with management, the Department's risk management framework incorporating, inter alia, the:
  - i. Risk management Policy
  - ii. Fraud Prevention Policy;
  - iii. Risk management strategy;
  - iv. Fraud Prevention strategy;
  - v. Risk management implementation plan;
  - vi. Risk identification and assessment methodology;
  - vii. Risk appetite and tolerance;
  - viii. Risk classification and etc.
- b) Facilitating the annual risk assessment process.
- c) Responsible for educating management and staff in the risk management process.
- d) Responsible for creating an awareness of risks, fraud prevention and assisting management in ensuring that there is a culture of effective controls.
- e) Monitoring and reporting to the Accounting Officer, Management and Risk Management Committee on the implementation of risk management
- f) Participating with Internal Audit, Management and Auditor-General in developing the combined assurance plan for the Department.
- g) Ensure that there is an effective communicative framework to all staff and outlying to consolidate the influence and efforts risk management. The use of internal circulars (signed by the Accounting Officer) or delegated officer) should form part of such framework.

The risk management function is not in place to manage specific risks on behalf of management. The function will play a co-ordination and facilitation role.

## **5.7 Other Employees**

Other employees are responsible for integrating risk management into their day-to-day activities.

High level responsibilities of other officials should include:

- a. Apply the risk management processes in their respective functions

- b. Implement the delegated action plans to address the identified risks
- c. Informing their supervisors and/ or Risk Management Unit of new risks and significant changes in known risks, non-compliance with the code of conduct, other policy violations or illegal actions
- d. Co-operate with other role players in the risk management process and providing information as required.

Risk Management is the responsibility of every official in the Department and therefore it should be an explicit and implicit part of everyone's job description. Virtually all personnel produce information used in risk management or take other actions needed to manage risks.

A number of external parties often contribute to the achievement of a Department's objectives. External parties which may provide information useful to the Department's effective risk management are regulators... External parties, however, are not responsible for the Department's risk management.

### **5.8 Internal Audit**

- a. Internal audit and other assurance providers will provide assurance to the Accounting Officer, Management, Risk Management Committee and the Audit Committee that adequate and effective risk management and control processes are in place throughout the Department.
- b. Internal auditors play an important role in the monitoring of risk management and the quality of performance as part of their regular duties or upon special request of senior management, which will be approved by the Audit Committee.
- c. Internal Audit may assist management, the Executive Authority and Accounting Officer by monitoring, examining, evaluating, reporting on and recommending improvements to the adequacy and effectiveness of management's risk management processes.
- d. Such request should however be routed through the Audit Committee to ensure that such involvement does not affect the completion of the approved audit plan
- e. External auditors bring an independent and objective view, contributing directly through the audit of financial statement and internal control examinations, and indirectly by providing additional information useful to management and the executive authority in carrying out their responsibilities.

### **5.9 Risk Champions**

Although it is acknowledged that management undertake (on behalf of the Accounting Officer) the sectional responsibility to ensure that risk is adequately managed within the specific strategic framework under his/her leadership, it is of extreme importance that the use of risk champions in respect of programs and outlying districts should be strongly supported and maintained to create a link of communicative guidance towards active and continuous fulfilment of risk prevention strategies and actions as well as a collective synergy with the aspirations and actions required from an effective risk containment

central unit.

It is therefore accepted that suitable candidates will be selected from each program, as well as outlying districts to perform the task of:

- a) Co-operating with the Chief Risk Officer/ delegated Risk Officer of the risk committee on all risk issues.
- b) Coordinating risk activities and contemplation forums to discuss relevant risk issues that may occur in that sector of control.
- c) Identify, recommend and facilitate training to all key role players within that control area.
- d) Illuminating the responsibilities of risk identification, conveyance and active prevention of all employees.
- e) Ensure that a proper understanding of the process and objectives is anchored with all staff through regular meetings and workshops.
- f) Ensure that all new risks are appropriately assessed and communicated to the Risk Committee for inclusion in the risk register.
- g) Ensure that succession planning forms an integral part within the risk control in order to maintain risk control efficiency.
- h) Monthly written report to the Chief Risk Officer on any risk related issues which may be included in the quarterly report to the Risk Committee?

Risk champions is to be appointed by way of a signed letter of appointment by the Accounting Officer, although no remuneration is attached to such ad hoc duties; most appraisals may be used for performance incentives.

### **5.10 Training**

Risk Management training will be made available to members, officers, champions and all relevant employees within the Department.

## **6. RISK MANAGEMENT PROCESS**

The risk management process will involve the following procedures:

- a) To define and implement a context for risk management in the Department by:
  - i) Creating an appropriate control environment of values, discipline and structure within the Department.
  - ii) Developing a centrally co-ordinated risk framework and management process to ensure consistency throughout the Department.

### **6.1 Risk Management**

- a. Ensuring that risk management is not one event, but a series of continuous actions that permeate a Department's activities.

- b. Defining the responsibility structure for risk management throughout the Department.
- c. Develop a clear and unambiguous understanding of our strategic objectives and purpose.
- d. Continually evaluating and reviewing the internal and external environment for risks that may affect the achievement of our strategic objectives.
- e. Continually reviewing our risk tolerance as our internal and external environment changes.

To implement the following continuous risk management process in the Department:

- f. An annual review the most significant risks facing the organisation.
- g. Assessment and evaluation of the inherent impact and likelihood of risk occurring.
- h. Determination of the Department's response to the risk – Take, Manage, Transfer (insure) or Avoid. Cost benefit as well as service delivery considerations will be a factor in deciding on the most suitable response.
- i. Where the response is to manage or transfer the risk, we will examine existing procedures and controls in place to manage the risk to an acceptable level.
- j. Re-evaluation of the risk after taking controls into account, to obtain the residual risk/ exposure.
- k. Consideration of any enhancements to control that may be required to reduce residual exposure to an acceptable level.
- l. Continual monitoring of the status of risks and develop a process for appropriate action if that status changes.
- m. Report to senior management and the audit committee on an ongoing basis regarding the results and status of risk management throughout the Department.
- n. Maintaining an awareness of risk and risk management processes throughout the Department.

The Risk Management Framework of the Department considered the following risk types and categories:

**FIGURE 1**

RISK CATEGORY	DESCRIPTION
<ul style="list-style-type: none"> <li>o Human resources</li> </ul>	<p>Risks that related to human resources of the Department. These risks can have an effect on an Department's human capital with regard to:</p> <ul style="list-style-type: none"> <li>• Integrity and Honesty</li> <li>• Recruitment</li> <li>• Skills and Competence</li> <li>• Employees wellness</li> <li>• Employees relations</li> <li>• Retention</li> <li>• Occupational health and safety</li> </ul>
<ul style="list-style-type: none"> <li>o Knowledge and Information Management</li> </ul>	<p>Risks relating to the Department's management of knowledge and information. In identifying the risks we should consider the following aspects related to knowledge management:</p> <ul style="list-style-type: none"> <li>• Availability of information</li> <li>• Stability of the information</li> <li>• Integrity of information data</li> <li>• Relevance of the information</li> <li>• Retention</li> <li>• Safeguarding</li> </ul>
<ul style="list-style-type: none"> <li>o Litigation</li> </ul>	<p>Risks that the Department might suffer losses due to litigations and lawsuits against it. Losses from litigation can possibly emanate from:</p> <ul style="list-style-type: none"> <li>• Claims by employees, the public, service providers and other third parties</li> <li>• Failure by the Department to exercise certain rights that are to its advantage</li> </ul>
<ul style="list-style-type: none"> <li>o Loss/theft of assets</li> </ul>	<p>Risks that the Department might suffer losses due to either theft or loss of an asset of the Department by employees</p>
<ul style="list-style-type: none"> <li>o Material resources (Procurement risk)</li> </ul>	<p>Risks relating to the Department's material resources. Possible aspects to consider include:</p> <ul style="list-style-type: none"> <li>• Availability of material</li> <li>• Costs and means of acquiring/ procuring resources</li> <li>• The wastage of material resources</li> </ul>
<ul style="list-style-type: none"> <li>o Service Delivery</li> </ul>	<p>The Department exists to provide value for its stakeholders. The risk will arise if the appropriate quality of service is not delivered to the Citizens.</p>





<p>o Information Technology</p>	<p>The risks relating specifically to the institution's IT objectives, infrastructure requirements, etc. possible considerations could include the following when identifying applicable risks:</p> <ul style="list-style-type: none"> <li>• Security concerns</li> <li>• Technology availability(uptime)</li> <li>• Applicability of IT infrastructure</li> <li>• Integration/interface of the systems</li> <li>• Effectiveness of technology</li> <li>• Obsolescence of technology</li> <li>• IT governance</li> </ul>
<p>o Third Party performance</p>	<p>Risks related to an institution's dependence on the performance of a third party. Risk in this regard could be the likelihood that a service provider might not perform according to the service level agreement entered into with an institution. Non-performance could include:</p> <ul style="list-style-type: none"> <li>• Outright failure to perform</li> <li>• Not rendering the required service in time</li> <li>• Not rendering the correct service</li> <li>• Inadequate/poor quality of performance</li> </ul>
<p>o Compliance/ Regulatory</p>	<p>Risks related to the compliance requirements that an institution has to meet. Aspects to consider in this regard are:</p> <ul style="list-style-type: none"> <li>• Failure to monitor or enforce compliance</li> <li>• Monitoring and enforcement mechanisms</li> <li>• Consequences of non-compliance</li> <li>• Fines and penalties paid</li> </ul>
<p>o Fraud and Corruption</p>	<p>These risks relate to illegal or improper acts by employees resulting in a loss of the institution's assets or resources.</p>
<p>o Financial</p>	<p>Risks encompassing the entire scope of general financial management. Potential factors to consider include:</p> <ul style="list-style-type: none"> <li>• Cash flow adequacy and management thereof</li> <li>• Financial losses</li> <li>• Wasteful expenditure</li> <li>• Budget allocations</li> <li>• Financial statement integrity</li> <li>• Revenue collection</li> <li>• Increasing operational expenditure</li> </ul>
<p>o Social environment</p>	<p>Risks relating to an institution's overall culture and its control environment. The various factors related to organisational culture include:</p> <ul style="list-style-type: none"> <li>• Communication channels and their effectiveness</li> <li>• Cultural integration</li> <li>• Entrenchment of ethics and values</li> <li>• Goal alignment</li> <li>• Management style</li> </ul>

o Reputation	Factors that could result in the tarnishing of an institution's reputation, public perception and image.
o Legislative environment	Risks related to the institution's legislative environment, for example changes in legislation, or conflicting legislation.
o Political environment	Risks emanating from political factors and decisions that have an impact on the institution's mandate and operations. Possible factors to consider include: <ul style="list-style-type: none"> <li>• Political unrest</li> <li>• Local, provincial and national elections</li> <li>• Changes in the office bearers</li> </ul>
o natural environment	Risks relating to the institution's natural environment and its impact on normal operations. Consider factors such as: <ul style="list-style-type: none"> <li>• Depletion of natural resources</li> <li>• Environmental degradation</li> <li>• Spillage</li> <li>• pollution</li> </ul>
o Economic environment	Risks relating to the institution's economic environment. Factors to consider include: <ul style="list-style-type: none"> <li>• Inflation</li> <li>• Foreign exchange fluctuations</li> <li>• Interest rates</li> </ul>
o Social environment	Risks related to the institution's social environment. Possible factors to consider include: <ul style="list-style-type: none"> <li>• Unemployment</li> <li>• Migration of workers</li> </ul>
o Technological environment	Risks emanating from the effects of advancements and changes in technology.
o Disaster Recovery	Risks related to an institutions preparedness or absence thereof for disasters that could impact the normal functioning of the institution, for example natural disasters, an act of terrorism etc. this would lead to the disruption of process and service delivery, and could include the possible disruption of operations at the onset of a crisis to the resumption of critical activities. Factors to consider include: <ul style="list-style-type: none"> <li>• Disaster management procedures</li> <li>• Contingency planning</li> </ul>
o Health and Safety	Risks from occupational health and safety issues, for example injury on duty or the outbreak of disease within the institution.

The Risk Management Strategy will be reviewed on an annual basis to ensure that it remains appropriate to the Department, and that the latest best practice of risk management has been adopted where appropriate.

In order to achieve the required strategic objectives, the Department might need to take certain risks. Management is responsible for understanding the level of risk which has

*nan*



been undertaken to achieve objectives, as well as the process in place to mitigate such risks.

Based on the need to balance the achievement of performance against the need to protect its stakeholders, the Department has approved the implementation of this risk strategy as a key component of Corporate Governance.

The risk management process needs to be integrated into the current processes within the Department.

## 6.2 The Risk Management Process consists of the following key stages:

### 6.2.1 Risk Profiling

- I. **Determination of objectives:** The objectives of a Department/ division should be identified along with the key performance indicators to measure the achievement of these objectives.
- II. **Identification of risks:** The risks which can prevent the achievement of the objectives will be identified. Identification of risks will use the skills and experience of management, in conjunction with established industry risk models. The risk model to be used has been included as Appendix B.
- III. **Risk Evaluation:** The impact and likelihood of risks, pre and post the considering the current systems, controls, processes and people in place will be assessed using the criteria in Appendix A. The outcome of this evaluation for each risk will be compared to the risk appetite to determine if the current exposure is acceptable, cautionary or unacceptable.
- IV. **Identification of opportunities:** For each objective and area profiled management should identify opportunities for improving current practices. These opportunities will then be subject to rigorous planning.

### 6.2.2 Review of Internal Controls

- I. **Revision of Control Strategy:** Once the initial risk profile has been completed for each area, management will review the control strategy for each individual risk to assess if it is the most appropriate. Control strategies which can be employed which these are:

**Retention:** low or tolerable risks may be accepted. This is normally the case for low impact risks with a low likelihood of occurrence. In accepting the risk the Department will continuously monitor the risk.

**Avoidance:** Certain new ventures, initiatives and / or projects may have too much associated risk and as such a decision can be taken not to engage in the activity.

**Transfer/Sharig:** In most cases the risks need to be managed, in a cost effective manner, so that the risk exposure is acceptable. This control strategy includes transferring the risk to a third party such as an outsourcing a function. Note the transfer of risks normally occurs for risks with a high impact but a low likelihood of occurrence.

**Control:** is the pro-active control of adverse consequences of a risk by implementing preventative measures. It is the risk, which is cost effective to control or treat.

- II. **Control Enhancements:** If the control strategy is to manage the risks, then the system of internal controls in place to manage the risks need to be reassessed. Improvements may be required to the systems of internal control and this would include identifying efficiency issues which can reduce the cost of control. To assist in this regard it should be noted that:
- III. **Preventative controls** which manage the likelihood of a risk occurring are more efficient than **detective controls** which manage the impact of the risks were they to occur. **Automated controls** are more efficient than **manual controls** and are generally more reliable.

Where improvements to the current internal control systems are required, action plans will be documented by management, and all internal control procedures for a section in the Department should be documented and used for training of officials.

### 6.2.3 Risk and Control Monitoring

- I. **Key Risk Indicators:** For each of the risks in the profiles, where appropriate, management will identify the key risk indicators which should be monitored to determine if the risk is likely to materialise. These key risks indicators will complement our key performance indicators and will be included in our management reporting.
- II. **Issue Tracking:** Where risks in the profile are identified as unacceptable or where control improvements are identified, management will track progress in resolving these issues until the revised internal controls are embedded in the operations.
- III. **Re-assessment of risks:** Some risks, by their nature, need to re-evaluate on a frequent basis and this period will be determined by management. However, as a minimum the risk profiles and system of internal control to manage the risks should be formally re-assessed on an annual basis.

### 6.2.4 Risk Register Record Keeping

The Risk Management Unit are the custodian of the Departmental Risk register of the Department, only the Chief Risk Officer can amend by adding or updating the Risk Register, as per the emerging risks.

### 6.2.5 Risk Management Reporting

The reporting of the risk management process should be through current reporting lines. The reporting process will be subject to change as the Department's requirements and risk management practices evolve. Basic protocols have been set out below:

Risk information that must be reported includes:

- a) Key risks – including the impact and likelihood pre control, controls in place to manage the risk and residual risk post control consideration.
- b) Any material changes to the risk profile.
- c) Summaries of significant control breakdowns/ losses.

- d) Breaches of controls or legal requirements
- e) The results of assurance work to date
- f) Reasons for breakdowns/ deviations and corrective action taken to minimise the risk.

Escalation procedures should be in place to ensure that appropriate material risk issues are reported timeously to the appropriate person. As documented above, the risk management process is being applied to strategic and operational risks as well as to new ventures, initiatives and / or projects.

However, the Accounting Officer recognises that there also needs to be a sound system of risk management and internal control in place at a process level. Management is accountable, as above, for ensuring that this is achieved.

However, it is not practical or cost effective to implement the above risk management process to all our processes throughout the Department.

As such at a process level the Accounting Officer relies on management control self-assessment whereby management take responsibility for asserting that the controls in place to manage the key process risks are adequate and have been effectively applied throughout the financial year.

The key process risks for each of the operations are discussed and agreed between management and internal audit and are reviewed and approved by the Audit Committee. Internal audit will base their internal coverage on the most significant risk areas identified through the risk assessment process.

The control self-assessment is complimented by the independent assurance provided by internal audit on the adequacy and effectiveness of the controls in place to manage the agreed key process risks.

Management is responsible for addressing areas of concern raised by Internal Audit and this is monitored by the Risk Management and Audit Committee.

## **APPENDIX A: DEFINITIONS AND CRITERIA FOR RISK EVALUATION**

### **1. DEFINITIONS**

#### **IMPACT**

This is potential magnitude of the impact on the Department's operations should the risk/threat actually occur.

This must be assessed on the basis that management have specific controls in place to address the risk/threat, i.e. without any controls in place, what will the impact of the risk be on the Department's ability to achieve its strategic and major objectives?

#### **1.1 THE PROBABILITY OF OCCURRENCE/ LIKELIHOOD**

This is the likelihood that the identified risk/threat will occur within a specified period of time (between 1 and 3 years) on the basis that there are no controls in place to address the risk/threat.

#### **1.2 INHERENT RISK**

Inherent risk is a product of impact and probability of occurrence. It is the Department's assessed maximum risk exposure before the implementation of any specific controls to reduce such exposure to risk

#### **1.3 CONTROL EFFECTIVENESS**

Control effectiveness refers to the control environment of the Department. The perceived effectiveness of controls is an indication of how well risks are managed.

#### **1.4 RESIDUAL RISK**

This is the value of risk that the Department is exposed after taking into account the *related controls* which currently are believed to be in place to manage that risk.

Residual risk/exposure is therefore the difference between the **assessed** inherent risk and the related control effectiveness.

#### **1.5 RISK APPETITE**

This means the amount of residual risk that the Department is willing to accept, although Government institutions are service delivery driven, its then create a dilemma on how should this institutions created the appetite and tolerant levels.

#### **1.6 CONTROL**

The control environment can be defined as "any action taken by management to enhance the likelihood that established objectives and goals will be achieved. Management plans, organises and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved. This control is the result of proper planning, organising and directing by management.

## 2. DESIRED CONTROL EFFECTIVENESS

Desired control effectiveness is the control effectiveness the Department is striving to achieve. This control effectiveness would enable the Department to reduce their risk exposure to the desired level.

### 2.1 CRITERIA FOR ASSESSING RISKS

In order to rank the identified risks, the following criteria are used:

(a) Likelihood ignoring existing controls (*the probability of the occurrence of the risk event*) and

(b) Impact ignoring existing controls (*the potential effect on the Department of the risk event*).

### 2.2 INHERENT RISK

Maximum risk exposure before the implementation of any specific controls to reduce such exposure to risk:

**FIGURE 2**

Rating scale	Likelihood	Interpretation
5	Almost Certain	The event is expected to occur in most circumstances
4	Likely	The event will probably occur in most circumstances
3	Moderate	The event should occur at some time
2	Unlikely	The event could occur at some time
1	Rare	The event may only occur in exceptional circumstances

### 2.3 RESIDUAL RISK

The effectiveness of the controls with regards to the Control effectiveness:

**FIGURE 3**

Risk Index	Risk Magnitude	Interpretation
0 to 5	Minimum	Minimum impacts on the Department's service delivery
6 to 9	Low	Significant impacts on the Department's service delivery
10 to 14	Medium	Medium impact on the Department's service delivery.
15 and 25	High	High/potential failure on the Department's service delivery.


Assessment is done using a scale of 1 to 5 (low to high). The following definitions are applied for the voting:

#### **2.4 RISK RATING**

##### **IMPACT:**

Impact is the potential loss to the Department (ignoring existing controls) should the risk materialise. Impact is rated on a scale of 1 to 5

Risk events will be assessed by analysing their impact and likelihood using the scales figure 4 below:



**FIGURE 4**

RATING	SEVERITY OF IMPACT	CONTINUITY OF SERVICE DELIVERY	SAFETY & ENVIRONMENTAL	TECHNICAL COMPLEXITY	FINANCIAL LOSSES
5	Critical	Risk event will result in widespread and lengthy reduction in continuity of service delivery to customers for a period greater 48 hours	Major environmental damage. Serious injury (permanent disability) or death of personnel or members of the public. Major negative media impact	Use of unproven technology for critical systems /project component. High level of technical interdependencies between system components	Can lead to termination of Business activity
4	Major	Reduction in service delivery or disruption for a period ranging between 24 & 48 hours over a significant area	Significant injury of personnel or public. Significant environmental damage. Significant negative media coverage	Use of new technology not previously utilized by the organization for critical systems/ project components	Cost increase 10 %
3	Moderate	Reduction in service delivery or disruption for a period ranging between 24 & 48 hours over a significant area	Lower level of environmental, safety or health impacts. Negative media coverage	Use of unproven or emerging technology for critical systems/ Project components.	Cost increase 5-10 %
2	Minor	Brief in service delivery or disruption for a period between 8 & 24 hours over a significant area	Little environmental, safety or health impacts. Limited negative media coverage	Use of unproven or emerging technology for critical systems /project components.	Cost increase 5-10 %
1	Insignificant	No disruption or impact on business or core systems	No environmental, safety or health impacts and /or negative media coverage	Use of unproven or emerging technology for non -critical systems /project components	Minimal or no impact on cost

22 *na*



**FIGURE 4**


EFFECTIVENESS CATEGORY	CATEGORY DEFINITION	Control Effectiveness %
Very Good	Risk exposure is effectively controlled and managed.	90%
Good	Majority of risk exposure is effectively controlled and managed.	80%
Satisfactory	There is room for some improvement.	60%
Weak	Some of the risk exposure appears to be controlled, but there are major deficiencies.	40%
Unsatisfactory	Control measures are inactive.	20%



**REVIEWAL OF THE STRATEGY**

The Risk Management Strategy shall be reviewed on to reflect the current stance on risk management.

**RECOMMENDED FOR APPROVAL**

  
\_\_\_\_\_  
**HEAD OF DEPARTMENT:**  
**MRS MOC MHLABANE**

12/09/2014  
\_\_\_\_\_  
**DATE**