

# SOL PLAATJE MUNICIPALITY



## ENTERPRISE RISK MANAGEMENT FRAMEWORK AND POLICY

Prepared by:

**SOL PLAATJE MUNICIPALITY RISK MANAGEMENT UNIT**

AND



*This document should be read in conjunction with the Risk Management Strategic Plan for Risk Management*

*The purpose of this document is to provide information and guidance to enable the implementation and maintenance of effective systems to identify and mitigate the risks that threaten the attainment of SPM's service delivery and other objectives, and to optimise opportunities that enhance institutional performance*

August 2010

Version 1

Enterprise Risk Management Framework

## Contents

1	Introduction	1
1.1	Background	1
1.2	Definitions	2
1.2.1	Risk	2
1.2.2	Enterprise Risk Management	2
1.2.3	Other definitions	2
1.3	Purpose of the Enterprise Risk Management Framework	3
1.4	Benefits of the Enterprise Risk Management Framework	4
1.5	Legal mandate	5
1.6	Corporate Governance Principles	6
2	Enterprise Risk Management Standards	7
3	Enterprise Risk Management Framework Guidelines	10
3.1	Roles, responsibilities and governance	10
3.1.1	Audit and Risk Committee	10
3.1.2	The Municipal Manager (MM)	12
3.1.3	The Executive Management Team (EMT)	13
3.1.4	The Risk Officer	14
3.1.5	Internal Audit	15
3.2	Risk Appetite	16
3.3	Components of the Enterprise Risk Management Process	18
3.3.1	Component 1 – Control Environment	19
3.3.2	Component 2 – Objective Setting	20
3.3.3	Component 3 – Risk Identification	20
3.3.4	Component 4 – Risk Assessment	26
3.3.5	Component 5 – Risk Response Strategy	29
3.3.6	Component 6 – Information and Communication	30
3.3.7	Component 7 – Control Activities	31
3.3.8	Component 8 – Monitoring	31
3.4	Governance requirements	33
3.4.1	Establish an organisational framework of assurance for key risks and controls	33
3.4.2	Internal audit provides assurance on risk management processes	34
3.4.3	The outputs of risk assessments are used to direct internal audit plans	34
3.4.4	Internal audit provides assurance on quality and reliability of risk information	34
3.4.5	Safety, health and environment	34
3.4.6	Business Continuity Management	34
3.4.7	Fraud Prevention and Anti-corruption Plan	35

# 1 Introduction

## 1.1 Background

Enterprise Risk Management (ERM) forms a critical part of any entity's strategic management. It is the process whereby an entity both methodically and intuitively addresses the risk attached to their activities with the goal of achieving sustained benefit within each activity and across a portfolio of activities. Enterprise Risk Management is therefore recognized as an integral part of sound organizational management and is being promoted internationally and in South Africa as good business practice applicable to the public and private sectors.

The underlying premise of enterprise risk management is that every entity exists to provide value for its stakeholders. All entities face uncertainty and the challenge for management is to determine how much uncertainty to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value.

Enterprise risk management enables management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value. Value is maximized when management sets strategy and objectives to strike an optimal balance between growth and return goals and related risks, and efficiently and effectively deploys resources in pursuit of the entity's objectives.

The framework provides a basis for management to effectively deal with uncertainty of associated risk and opportunity, thereby enhancing its capacity to build value.

The following factors require consideration when integrating ERM into organisational decision making structures:

- Aligning risk management with objectives at all levels of the organisation;
- Introducing risk management components into existing strategic planning and operational practices;
- Including risk management as part of employees' performance appraisals; and
- Continuously improving control and accountability systems and processes to take into account risk management and its results.

The Enterprise Risk Management Framework specifically addresses the structures, processes and standards implemented to manage risks on an enterprise-wide basis in a consistent manner. The standards further address the specific responsibilities and accountabilities for the Enterprise Risk Management process and the reporting of risks and incidences at various levels within SPM. As the field of risk management is dynamic, this policy and framework document is expected to change from time to time.

Current trends in good corporate governance have given special prominence to the process of Enterprise Risk Management and reputable businesses are required to demonstrate that they comply with expected risk management standards. This means that SPM must ensure that the process of risk management receives special attention throughout the organisation and that all levels of management know, understand and comply with the framework document.



## 1.2 Definitions

### 1.2.1 Risk

The Institute of Internal Auditors defines risk as “...*the uncertainty of an event occurring that could have an impact on the achievement of objectives. Risk is measured in terms of consequences and likelihood.*”

### 1.2.2 Enterprise Risk Management

With reference to the highly accepted COSO framework (The Committee of Sponsoring Organisations of the Treadway Commission):

*“Enterprise risk management is a continuous, proactive and systematic process, effected by the Board of Directors, Executive Management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity’s objectives.”*

The definition reflects certain fundamental concepts. Enterprise risk management should be:

- A process, ongoing and flowing through SPM
- Effected by people at every level of SPM
- Applied in strategy setting
- Applied across the organisation, at every level and unit, and includes taking a group level portfolio view of risk
- Designed to identify potential events that, if they occur, will affect SPM and to manage risk within SPM’s risk appetite
- Able to provide reasonable assurance to SPM’s management and the Audit and Risk Committee
- Geared to achieve objectives in one or more separate, but overlapping categories.

### 1.2.3 Other definitions

#### **Accounting officer**

The Municipal Manger

#### **Audit and Risk Committee**

An independent committee constituted to review the control, governance and risk management within the institution, established in terms of section 166 of the MFMA.

#### **Risk Officer**

A senior official who is the head of SPM's Risk Management Unit.

#### **Executive Authority**

The Municipal Council, led by the Executive Mayor.



**Framework**

The Enterprise Risk Management Framework.

**Inherent Risk**

The exposure arising from risk factors in the absence of deliberate management intervention(s) to exercise control over such risk factors.

**Internal Audit**

An independent, objective assurance and consulting activity designed to add value and improve SPM's operations. It helps SPM to accomplish its objectives by bringing a systematic, disciplined approach to evaluating and improving the effectiveness of risk management, control, and governance processes.

**MFMA**

Municipal Finance Management Act (No. 56 of 2003).

**Residual Risk**

The remaining risk exposure after the mitigating effects of deliberate management intervention(s) to control such risk exposure.

**Risk Appetite**

The extent of willingness to take risks in the pursuit of the business objectives.

**Risk Champion**

A person who by virtue of his/her expertise or authority champions a particular aspect of the risk management process, but who is not necessarily the risk owner.

**Risk Factor (Contributory Factor)**

Any threat or event which contributes to the risk materialising, or has the potential to contribute to the risk materialising.

**Risk Management Committee**

Role fulfilled by the Executive Management Team (EMT).

The committee responsible for designing, implementing and monitoring the process of risk management and integrating it into the day-to-day activities of SPM.

**Risk Management Unit (RMU)**

A SPM business unit responsible for coordinating and supporting the overall institutional risk management processes, but which does not assume the responsibilities of identifying, assessing and managing the risks.

**Risk Owner**

The person accountable for managing a particular risk.

**Risk Tolerance**

The level of risk exposure the institution is willing to bear.

**1.3 Purpose of the Enterprise Risk Management Framework**

The purpose of the Enterprise Risk Management Framework is to:



- Advance the development and implementation of modern management practices and to support innovation throughout SPM;
- Contribute to building a risk-smart workforce and environment that allows for innovation and responsible risk-taking while ensuring legitimate precautions are taken to protect the public interest, maintain public trust, and ensure due diligence;
- Provide a comprehensive approach to better integrate risk management into strategic decision-making; and
- Provide guidance for the Executive Authority, Accounting Officer, Managers and staff when overseeing or implementing the development of processes, systems and techniques for managing risk, which are appropriate to the context of SPM.

## 1.4 Benefits of the Enterprise Risk Management Framework

The benefits of the Enterprise Risk Management Framework are as follows:

- **Aligning risk appetite and strategy** – SPM's management will consider their risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks.
- **Pursuing business objectives through transparent identification and management of acceptable risk** – There is a direct relationship between objectives, which are what an entity strives to achieve and the enterprise risk management components, which represent what is needed to achieve the objectives.
- **Providing an ability to prioritise the risk management activity** – Risk quantification techniques assist management in prioritizing risks to ensure that resources and capital are focussed on high priority risks faced by the entity.
- **Enhancing risk response decisions** – Enterprise Risk Management provides the basis for management to identify and select alternative risk responses –transfer the risk, tolerate, treat, or terminate.
- **Reducing operational surprises and losses** – SPM will gain enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses.
- **Identifying and managing multiple and cross-enterprise risks** - SPM faces a myriad of risks affecting different areas of its business activities and Enterprise Risk Management facilitates an effective response to the interrelated impacts, and an integrated responses to the multiple risks.
- **Seizing opportunities** - By considering a full range of potential events, SPM management will be in a position to identify and proactively realize opportunities.
- **Improving deployment of capital** - Obtaining robust risk information allows SPM management to effectively assess overall capital needs and enhance capital allocation.
- **Ensuring compliance with laws and regulations** – Enterprise Risk Management helps to ensure effective reporting and compliance with laws and regulations, and helps to avoid damage to SPM's reputation and associated consequences.
- **Increasing probability of achieving objectives** – Enterprise Risk Management assists management in achieving SPM's objectives and prevents loss of resources. Controls and risk



interventions will be chosen on the basis that they increase the likelihood that SPM will fulfil its undertakings to stakeholders.

## 1.5 Legal mandate

### MFMA

Section 62.(1)(a) of the MFMA states that “The accounting officer of a municipality is responsible for managing the financial administration of the municipality, and must for this purpose take all reasonable steps to ensure that the municipality has and maintains effective, efficient and transparent systems of financial and risk management and internal control...”

### Treasury Regulations

Section 3.2.1 of the Treasury Regulations states the following:

“The accounting officer must ensure that a risk assessment is conducted regularly so as to identify emerging risks of the institution. A risk management strategy, which must include a fraud prevention plan, must be used to direct the internal audit effort and priority ...”



## 1.6 Corporate Governance Principles

The following recommendations are made in Section 3 of the King III Report on Governance Principles for South Africa:

- The Audit and Risk Committee is responsible for the total process of risk management, as well as forming its own opinion on the effectiveness of the process.
- The Audit and Risk Committee should consider the risk strategy and policy, and should monitor the process at operational level and the reporting thereon. The Audit and Risk Committee should also consider the results of the risk management and internal control processes and the disclosure thereof.
- Management is accountable to the Audit and Risk Committee for designing, implementing and monitoring the process of risk management and integrating it into the day-to-day activities of the department.
- Risk Management constitutes an inherent operational function and responsibility.
- Risks should be assessed on an on-going basis and control activities should be designed to respond to risks throughout the company. Pertinent information arising from the risk assessment, and relating to control activities should be identified, captured and communicated in a form and timeframe that enables employees to carry out their responsibilities properly. These controls should be monitored by both line management and assurance providers.
- A systematic, documented assessment of the processes and outcomes surrounding key risks should be undertaken at least annually.
- The institution should develop a system of risk management and internal control that builds robust business operations. The systems should demonstrate that the key risks are being managed in a way that enhances shareowners' and relevant stakeholders' interests. The system should incorporate mechanisms to deliver:
  - i. a demonstrable system of dynamic risk identification;
  - ii. a commitment by management to the process;
  - iii. a demonstrable system of risk mitigation activities;
  - iv. a system of documented risk communications;
  - v. a system of documenting the costs of non-compliance and losses;
  - vi. a documented system of internal control and risk management;
  - vii. an alignment of assurance of efforts to the risk profile; and
  - viii. a register of key risks that could affect shareowner and relevant stakeholder interests.



## 2 Enterprise Risk Management Standards

The standards constitute the main tasks of the ERM process. These standards are non-negotiable.

The Enterprise Risk Management Standards should be read in conjunction with section 3 - ERM guidelines.

Ref.	Standard	Responsibility	Frequency
<b>Oversight Responsibilities:</b>			
01	The Audit and Risk Committee will review risk management progress at least quarterly.	Chairperson	Quarterly
02	The Executive Management Committee (EMT) will review risk management progress at least quarterly.	MM	Quarterly
03	The EMT will oversee the implementation of ERM and will meet monthly. Risk management should be a standing agenda item for all meetings of the EMT.	MM	Monthly
<b>Reporting Responsibilities:</b>			
04	The EMT will submit risk management reports to the Audit & Risk Committee on a quarterly basis. These reports will focus on the following: <ul style="list-style-type: none"> <li>• The strategic risks;</li> <li>• Progress with implementing corrective actions per risk;</li> <li>• Any new and emerging risks, risk developments, including incidents.</li> </ul>	MM and Risk Officer	Quarterly
<b>Risk Assessment Responsibilities:</b>			
05	The MM will ensure that a complete review of the risks of SPM is done at least once a year.	MM	Annually
06	Executive Directors and Senior Managers will review the risk registers and update the registers' contents to reflect any changes without the need to formally reassessment of the risks.	All Executive Directors and Senior Managers	Monthly



Ref.	Standard	Responsibility	Frequency
<b>Risk Mitigation Responsibilities:</b>			
07	The Audit & Risk committee will receive and consider management's report concerning the effectiveness of internal controls on a quarterly basis	Chairperson	Quarterly
08	The EMT will consider Executive Directors' and Senior Managers' reports regarding the performance of internal controls for those risks in the risk register which they are responsible for.	MM	Monthly
09	The risk register will contain action plans for improving risk controls and risk interventions. Progress in implementing these actions should be monitored.	Executive Directors and Risk Officer	Monthly
<b>Governance Responsibilities:</b>			
10	Each risk will have a nominated owner, who will be responsible for the following: <ul style="list-style-type: none"> <li>• Updating the risk information;</li> <li>• Providing assurance regarding the risk controls;</li> <li>• Coordinate the implementation of action plans for managing the risk;</li> <li>• Reporting on any developments regarding the risk.</li> </ul>	MM; Executive Directors and Senior Managers	Monthly
11	Internal Audit will use the outputs of risk assessments to compile the internal audit plan, and will investigate the effectiveness of risk mitigating controls.	Head of Internal Audit	Per approved IA plan
12	The Audit & Risk Committee will facilitate a review of the effectiveness of the entity's risk management processes.	Chairperson	Annually
13	A Business Continuity Plan will be developed, implemented and tested annually to ensure continuous maintenance.	MM and Manager: Policy	Annually



Ref.	Standard	Responsibility	Frequency
14	The Fraud Prevention and Anti Corruption plan should be implemented and monitored. Monthly incidents should be reported to the MM.	MM and CFO	Monthly



## 3 Enterprise Risk Management Framework Guidelines

The Enterprise Risk Management Framework ensures that key risks are identified, measured and managed. The Framework provides management with proven risk management tools that support their decision-making responsibilities and processes, while managing risks which impact on the attainment of SPM's objectives.

SPM has determined that Enterprise Risk Management is everyone's responsibility and that it must be embedded into the everyday activities of the organisation. This implies that Enterprise Risk Management must be part of every decision that is made, every objective that is set and every process that is designed. Enterprise Risk Management responsibilities for key risk management role players are detailed below.

### 3.1 Roles, responsibilities and governance

- All employees the Council of SPM have some responsibility for Enterprise Risk Management.
- The MM is ultimately responsible for Enterprise Risk Management and should assume overall ownership.
- The other managers support the risk management philosophy, promote compliance with the risk appetite and manage risks within their spheres of responsibility consistent with risk tolerances.
- Other personnel are responsible for executing Enterprise Risk Management in accordance with established directives and protocols.
- The Audit and Risk Committee provides important Enterprise Risk Management oversight.
- A number of external stakeholders often provide information useful in effecting Enterprise Risk Management, but they are not responsible for the effectiveness of SPM's Enterprise Risk Management.

#### 3.1.1 Audit and Risk Committee

##### 3.1.1.1 *Responsibilities for enterprise risk management*

The Audit and Risk Committee is responsible for the oversight of:

- The total process of risk management, which includes a related system of internal control;
- For forming its own opinion on the effectiveness of the process;
- Providing monitoring, guidance and direction in respect of Enterprise Risk Management;
- Ascertaining the status of enterprise risk management within SPM and providing oversight with regards to Enterprise Risk Management.
- Identifying and fully appreciating the risk issues and key risk indicators affecting the ability of SPM to achieve its objectives;
- Ensuring that appropriate systems are implemented to manage the identified risks, by measuring the risks in terms of impact and probability, together with proactively managing the mitigating actions to ensure that SPM's assets and reputation are suitably protected;



- Ensuring that SPM's Enterprise Risk Management mechanisms provide it with an assessment of the most significant risks relative to strategy and objectives;
- Considering input from the internal auditors, external auditors and subject matter specialists regarding Enterprise Risk Management;
- Utilising resources as needed to conduct special investigations and having open and unrestricted communication with management, internal audit and the external auditors;
- For disclosures in the annual report regarding Enterprise Risk Management;

Each member of the Audit & Risk Committee must understand his/her accountability for enterprise risk management within SPM. Although the Audit & Risk Committee may choose to nominate one member of the committee as the coordinator of enterprise risk management reporting requirements, it is clear that all members have accountability for Enterprise Risk Management in SPM.

### **3.1.1.2 *Providing stakeholder assurance***

In providing stakeholders with assurance that key risks are properly identified, assessed, mitigated and monitored the Audit & Risk Committee must:

- Receive credible and accurate information regarding the risk management processes within SPM in order to give the necessary assurance to stakeholders. The reports must provide an evaluation of the performance of risk management and internal control;
- Ensure that the various processes of Enterprise Risk Management cover the entire spectrum of risks faced by SPM. The assurance process includes statements regarding the appropriateness of SPM's risk/ reward trade-off;
- Provide stakeholders with the assurance that management has a pro-active approach to risk. It is vital that the management of risk is undertaken in a formalised manner.

### **3.1.1.3 *Maintenance of the ERM policy***

It is appreciated that stakeholders need to understand the Audit & Risk Committee' standpoint on risk. The Audit & Risk Committee will therefore maintain SPM's formal risk management policy, which decrees SPM's approach to risk and underpins the development of SPM's Enterprise Risk Management processes. The policy can be used as a reference point in matters of dispute and uncertainty.

### **3.1.1.4 *Assessing reasonableness of risk tolerance levels***

The Audit & Risk Committee will assess the reasonableness of SPM's levels of risk tolerance set by management. Risk tolerance limits are vital, because they determine and influence the decision making processes. Tolerance levels are set in relation to stakeholder expectations. Limits may be expressed in a number of ways according to the category of risk concerned. The establishment of risk tolerance limits shapes the exception reporting processes. Risk tolerance limits will be determined in accordance with the risk-taking propensity of SPM and the organisational culture of risk acceptability. The outcomes of risk assessment processes will assist the Audit & Risk Committee in assessing the reasonableness of the risk tolerance limits.



### **3.1.1.5 *Evaluating the effectiveness of the risk management process***

The Audit & Risk Committee will facilitate the evaluation of the effectiveness of SPM's Enterprise Risk Management processes on an annual basis.

It is recognised that Enterprise Risk Management has evolved into a complex management discipline in its own right. The Audit & Risk Committee' evaluation of risk management, therefore, will be supplemented by an independent review to be performed by National Treasury or other such nominated assurance provider. The annual review will be undertaken by qualified persons, with the ability to review all aspects of risk management.

Management must ensure that sufficient independence is maintained in conducting the annual review. Criteria for the evaluation must be established. Assurance of the processes surrounding key risks must be given.

### **3.1.1.6 *Confirming that the Enterprise Risk Management process is accurately aligned to the strategy and business objectives of SPM***

The Audit & Risk Committee will ensure that the Enterprise Risk Management processes address risk in a balanced way, giving due attention to all types of risk. The Audit & Risk Committee will evaluate whether appropriate resources are being applied to the management of the various categories of risk. The Audit & Risk Committee will evaluate whether risk management processes are aligned to the strategic and business objectives of SPM. A balanced perspective of risk and risk management is required in proportion to the weighting of potential risk impact across SPM. The Audit & Risk Committee must ensure that a future-looking orientation is included in the consideration of risk.

## **3.1.2 The Municipal Manager (MM)**

The MM's responsibilities include ensuring that all components of enterprise risk management are in place. The MM fulfils this duty by:

- Providing leadership and direction to management and staff. The MM shapes the values, principles and major operating policies that form the foundation of SPM's Enterprise Risk Management. The Council, MM, Executive Directors and Senior Managers set strategic objectives and strategy. They also set broad-based policies and develop SPM's Enterprise Risk Management philosophy, risk appetite and culture. They take actions concerning SPM's organisational structure, content and communication of key policies and the type of planning and reporting systems that SPM will use.
- Meeting periodically with Executive Directors and Senior Managers responsible for major business units and functional areas to review their responsibilities, including how they manage risk. The MM must gain knowledge of risks inherent to the municipal operations, risk responses and control improvements required and the status of efforts underway. To discharge this responsibility, the MM must clearly define the information he needs.

The MM is required to assess SPM's Enterprise Risk Management capabilities, as he has ultimate ownership and responsibility for Enterprise Risk Management. One of the most important aspects of this responsibility is ensuring the presence of a positive internal environment. More than any other individual or function, the MM sets the tone at the top that influences internal environmental factors and other components of Enterprise Risk Management.



The MM has been appointed to provide direction, guidance, support and to monitor Executive Directors and Senior Managers in effecting Enterprise Risk Management.

### 3.1.3 The Executive Management Team (EMT)

The EMT will fulfil the role of the Risk Management Committee. The EMT is accountable to the Audit & Risk Committee for designing, implementing and monitoring the process of risk management and integrating it into the day-to-day activities of SPM.

More specifically management is responsible for:

- Designing an Enterprise Risk Management programme in conjunction with the Risk Officer;
- Deciding on the manner in which risk mitigation will be embedded into management processes;
- Creating a culture of risk management within SPM ;
- Updating risk registers and providing risk management reports to the Risk Officer pertaining to risk and control;
- Identifying positive aspects of risk that could evolve into potential opportunities for SPM by viewing risk as an opportunity, by applying the risk/ reward principle in all decisions impacting on SPM;
- Taking responsibility for appropriate mitigation action and determining action dates;
- Utilising available resources to compile, develop and implement plans, procedures and controls within the framework of SPM's Enterprise Risk Management Policy to effectively manage the risks within SPM;
- Ensuring that adequate and cost effective risk management structures are in place;
- Identifying, evaluating and measuring risks and where possible quantifying and linking each identified risk to key risk indicators;
- Developing and implementing risk management plans including:
  - actions to optimise risk/ reward profile, maximise reward with risk contained within the approved risk appetite and tolerance limits;
  - implementation of cost effective preventative and contingent control measures; and
  - implementation of procedures to ensure adherence to legal and regulatory requirements.
- Monitoring of the Enterprise Risk Management processes on both a detailed and macro basis by evaluating changes, or potential changes to risk profiles;
- Implementing and maintaining adequate internal controls and monitoring the continued effectiveness thereof;
- Implementing those measures as recommended by the internal and external auditors, which, in their opinion, will enhance control at a reasonable cost;
- Reporting to the Audit and Risk Committee on the risk process and resultant risk/ reward profiles;
- Defining roles, responsibilities and accountabilities at Executive Directors and Senior Managers; and
- Providing policies, frameworks, methodologies and tools to the business units and key functional areas for identification, assessment and management of risks.



### 3.1.4 The Risk Officer

The Risk Officer is responsible for:

- Deciding on a methodology and framework for Enterprise Risk Management;
- Undertaking a Gap Analysis of the entity's Enterprise Risk Management process at regular intervals;
- Performing reviews of the risk management process to improve the existing process;
- Facilitating risk assessments;
- Developing systems to facilitate risk monitoring and risk improvement;
- Ensuring that all risk categories are included in the risk assessment;
- Ensuring that key risk indicators are included in the risk register;
- Aligning the risk identification process with SPM's business objectives;
- Obtaining agreement on a system of risk quantification;
- Identifying relevant legal and regulatory compliance requirements;
- Compiling a consolidated risk register on an annual basis;
- Costing and quantifying actual non-compliance incidences and losses incurred and formally reporting thereon;
- Formally reviewing the occupational health, safety and environmental policies and practices;
- Creating mechanisms for identifying modes of change;
- Consolidating all information pertaining to all risk related functions, processes and activities;
- Transferring the knowledge in respect of an effective and sustainable process of risk identification, quantification and monitoring to management;
- Recording the decisions regarding mitigation for every key risk facing SPM in the risk register;
- Deciding upon central solutions for common risks and for risks where central facilities are available;
- Liaising closely with Internal Audit to devise a risk auditing programme, based on the information reflected in the risk registers;
- Benchmarking the performance of the risk management process to the risk management processes adopted by other public entities within South Africa;
- Implementing a formalised risk information system;
- Ensuring that risk management training is conducted at appropriate levels within the entity to inculcate a risk management culture;
- Assisting in compiling risk registers for all functional areas at strategic, operational and project levels;
- Communicating the risk framework and methodology to all management levels and to employees;
- Ensuring that the necessary risk management documentation is developed in respect of the risk management process;
- Enabling the Audit & Risk committee to fulfil its responsibilities with regards to risk management;
- Communicating and managing the establishment and ongoing maintenance of enterprise risk management pursuant to SPM's risk management vision;



- Ensuring proper risk management ownership by responsible managers;
- Validating that enterprise risk management is functioning in all functional areas and that all significant risks are being recognised and effectively managed on a timely manner;
- Communicating with the Audit & Risk committee regarding the status of Enterprise Risk Management;
- Developing integrated procedures to report major risks;
- Developing a standardised risk information model and automated process and ensuring it is usable across SPM;
- Maintaining a cost-benefit focus on Enterprise Risk Management;
- Working with management to ensure business plans and budgets include risk identification and management.

### 3.1.5 Internal Audit

The role of Internal Audit in corporate governance is defined by the South African Institute of Chartered Accountants as follows: “To support the Board and Management in identifying and managing risks and thereby enabling them to manage the organisation effectively”. This is achieved by:

- Enhancing their understanding of risk management and the underlying concepts;
- Assisting them to implement an effective risk management process, and
- Providing objective feedback on the quality of organisational controls and performance.”

Internal Audit is responsible for:

- Providing assurance that management processes are adequate to identify and monitor significant risks;
- Using the outputs of risk assessments to direct internal audit plans;
- Providing ongoing evaluation of the risk management processes;
- Providing objective confirmations that the MM and Audit and Risk Committee receive the right quality of assurance and reliable information from management regarding risk;
- Providing assurance regarding Enterprise Risk Management processes from both a design and functional perspective;
- providing assurance regarding the effectiveness and efficiency of risk responses and related control activities; and
- Further providing assurance as to the completeness and accuracy of Enterprise Risk Management reporting.



## 3.2 Risk Appetite

***Risk appetite is defined as the extent of willingness to take risks in the pursuit of the business objectives.***

SPM may consider risk appetite qualitatively, with such categories as high, moderate or low, or they may take a quantitative approach, reflecting and balancing goals for capital expenditure, budgets and risk.

SPM's risk appetite guides resource allocation. Management allocates resources across departments and functional areas within departments with consideration to SPM's risk appetite and individual strategy for ensuring that expenditure remains within the budget of SPM and that the objectives are met. Management considers its risk appetite as it aligns its resources and designs infrastructure necessary to effectively respond to and monitor risks.

### ***Risk appetite:***

- Enables an improved consistency of decision making at all levels through improving risk understanding;
- Provides a framework for knowingly taking risk within defined boundaries;
- Improves the ability of the Audit & Risk Committee to challenge recommendations of management by providing a benchmark of what level of risk is defined as acceptable; and
- Derives real value from the assessment of risk over and above compliance purposes.

The risk appetite decided upon should be formally considered as part of the setting of business strategy, with capital expenditure and other strategic decisions reviewed against it as they arise.

As risk appetite is unlikely to be reduced to a single measurement, SPM needs to decide on the key measurements of risk that are best aligned to its business objectives and in most cases risk appetite will be defined by a mixture of quantitative and qualitative elements.

The key determinants of risk appetite are as follows:

- Expected performance;
- The resources needed to support risk taking;
- The culture of SPM;
- Management experience along with risk and control management skills;
- Longer term strategic priorities;

The formulation of the risk appetite is typically closely aligned to the strategic planning process and is also inclusive of budgeting, and as such is something that should be reviewed by management annually.

The Audit & Risk Committee reviews the Strategic Business Plan of SPM and approves the operating objectives as being achievable, within the context of the level of risk acceptable to SPM as part of the annual strategy approval process. SPM's risk appetite then represents the amount of risk SPM is willing to accept as it seeks to achieve its business objectives.

Risk appetite is communicated through the strategic and implementation plans at both organisational and operational levels. The Audit & Risk Committee and management will monitor the risk appetite of SPM relative to SPM's actual results and communicate any actions required as a result.



SPM reflects its Risk Appetite at an operational level through its Delegations of Authority to management. These delegated limits are made in respect of both financial and non-financial matters, which are then further delegated within each department and functional area.

The following risk appetite diagnostics may be considered:

- Cash flow;
- Development events;
- Clarity of strategy;
- Risk-taking propensity of management;
- Resources at risk;
- Exposure to market forces;
- Investment in Information Technology;
- Stagnation corrections/interventions;
- Customer orientation of service design; and
- Internal and external rate of change.



### 3.3 Components of the Enterprise Risk Management Process

A holistic approach to Enterprise Risk Management is required. This entails a coordinated enterprise-wide approach in which all risks are considered for the entire organisation and its departments. This approach includes all role players, policies, protocols, methodologies, reporting requirements and deliverables interacting within the Enterprise Risk Management processes.

The implementation of enterprise-wide risk management is guided by the methodology outlined in this document. The methodology is aligned to the **COSO** best practice as well as the National Treasury Risk Management Framework. The methodology allows for a consistent approach to be applied throughout SPM and facilitates the interaction, on risk management matters.



### 3.2.1 Component 1 – Control Environment

SPM's control environment is the foundation of risk management, providing discipline and structure. The control environment influences how strategy and objectives are established, SPM activities are structured, and risks are identified, assessed and acted upon. It influences the design and functioning of control activities, information and communication systems, and monitoring activities.

The control environment comprises many elements, including SPM's ethical values, competence and development of personnel, management's operating style and how it assigns authority and responsibility.

The executive authority is a critical part of the control environment and significantly influences other control environment elements. As part of the control environment, management establishes a risk management philosophy, establishes SPM's risk tolerance levels, inculcates a risk culture and integrates risk management with related initiatives.

The control environment consists of ten different layers that should all be present and functioning. The ten layers are as follows:

- Risk Management Philosophy

The risk management philosophy encompasses the tone set by SPM with respect to its risk appetite or risk tolerance, thereby implementing the basis for how risk is viewed and addressed.

The overall risk philosophy of SPM is to identify, assess and manage its business risks so as to preserve its strategic objectives. Given the return and growth objectives of SPM and the size of its operations, it is usually not possible to totally avoid all forms of risk. Therefore, SPM will accept, reduce or share risk provided that the residual exposure accepted is within the risk appetite or tolerance of SPM as this appetite manifests itself from time to time.

The overall aim is for Enterprise Risk Management to become embedded into all the critical systems and processes of SPM and to form an integral part of good management practices. Assurance processes focus on improving SPM's ability to manage risk effectively, so that SPM can respond confidently and in a timely manner to opportunities, creating stakeholder value.

- Risk tolerance
- Risk culture
- Executive Authority
- Integrity and values
- Commitment to competence
- Management's philosophy and operating Style
- Organisational structure
- Authority and responsibility
- HR policies and procedures

The existing controls in place for identified risks must be documented. The term "control" should not be construed only as a financial term. It is now the commonly accepted term to describe any mitigating measure for any particular type of risk. Controls may take the form of financial mitigations such as hedges, insurance or securities. They may be managerial in nature such as compliance



procedures, policies and levels of authority. Controls may be strategic in nature such as diversification and investment related. Controls may be legal such as contracts and indemnities.

### 3.2.2 Component 2 – Objective Setting

Objectives must exist before management can identify events potentially affecting their achievement. Risk management ensures that management has a process in place to both set objectives and align the objectives with SPM's mission and vision and is consistent with SPM's risk tolerance. The setting of these objectives is usually completed during the, "Strategic planning and Budgetary process."

The SPM objectives can be viewed in the context of five categories:

**Strategic** – relating to high-level goals, aligned with and supporting SPM's mission and vision;

**Operations** – relating to effectiveness and efficiency of SPM's operations, including performance and service delivery goals. They vary based on management's choices about structure and performance;

**Reporting** – relating to the effectiveness of SPM's reporting. They include internal and external reporting and may involve financial or non-financial information;

**Compliance** – relating to SPM's compliance with applicable laws and regulations;

**Safeguarding of assets** – relating to prevention of loss of a SPM's assets or resources, whether through theft, waste or inefficiency. Where the safeguarding concept applies to the prevention or timely detection of unauthorized acquisition, use, or disposition of SPM's assets.

This categorization of SPM objectives allows management and the executive authority to focus on separate aspects of risk management, although overlapping of the objectives when processes are managed is almost always applicable. Having confirmed and clearly documented SPM objectives, it is necessary to identify all the potential risks and threats relating to processes, assets and strategy. These are the possible problems and situations that may hinder the achievement of the objectives of the operation.

### 3.2.3 Component 3 – Risk Identification

During the phase of risk identification, management considers external and internal, as well as financial and non financial factors that influence the entity's policy and management agenda. Identifying major trends and their variation over time is particularly relevant in providing early warnings.

Some external factors to be considered for potential risks include:

- Political: the influence of international governments and other governing bodies;
- Economic: international, national markets and globalizations;
- Social: major demographic and social trends, level of citizen engagement; and
- Technological.



Internal factors reflect management's choices and include such matters as:

- The overall management framework;
- Governance and accountability frameworks;
- Level of transparency required;
- Values and ethics;
- Infrastructure;
- Policies, procedures and processes;
- Human resource capacity; and
- Technology.

An entity's risk identification methodology may comprise a combination of techniques together with supporting tools. Risk identification techniques look to both the past and the future. Techniques that focus on past events and trends consider such matters as payment default histories, overspending patterns, fraud and corruption and historic poor service delivery. Techniques that focus on future exposures consider such matters as shifting demographics, new laws and regulations and the impact of HIV on the resident population.

It may be useful to group potential events into categories. By aggregating events horizontally across an entity and vertically within operating units, management develops an understanding of the interrelationships between events, gaining enhanced information as a basis for risk assessment.

Events potentially either have a negative impact, a positive impact or both. Events that have a potentially negative impact represent risks, which require management's assessment and response. Accordingly, risk is defined as the possibility that an event will occur and adversely affect the achievement of objectives.

Events with a potentially positive impact represent opportunities or offset the negative impact of risks. Those representing opportunities are channelled back to management's strategy or objective-setting processes, so that actions can be formulated to seize the opportunities, whereas events potentially offsetting the negative impact of risks are considered in management's risk assessment and response.

#### **Possible methods of identifying risks:**

- Interview/focus group discussion;
- Audits or physical inspections;
- Brainstorming;
- Survey, questionnaires, Delphi technique;
- Examination of local and/or overseas experience;
- Networking with peers, industry groups and professional associations;
- Judgmental – speculative, conjectural, intuitive;



- history, failure analysis;
- Examination of past SPM and other public entity experiences;
- Incident, accident and injury investigation;
- Databank of risk events which have occurred;
- Scenario analysis;
- Decision trees;
- Strengths, weaknesses, opportunities, threats (SWOT) analysis;
- Flow charting, system design review, systems;
- Analysis, systems engineering techniques e.g. Hazard and Operability (HAZOP) studies;
- Work breakdown structure analysis; and
- Operational modelling.

#### **Possible Sources of Risk**

- New activities and services;
- Disposal or cessation of current activities;
- Outsourcing to external service providers;
- Commercial/legal changes;
- Changes in the economic conditions;
- Socio-political changes, like elections;
- Political interventions;
- National and international events;
- Personnel/human behaviour;
- Behaviour of contractors/private suppliers;
- Financial/market conditions;
- Management activities and controls;
- Misinformation;
- Technology/technical changes, i.e. new hardware and software implementations;
- Operational (the activity itself) changes;
- Service delivery interruption;
- Occupational health and safety;
- Property/assets;
- Security (including theft/fraud/impersonation);
- Natural events;
- Public/professional/product liability

#### **Possible Areas of Risk Impact**



A risk assessment should concentrate on all significant possible areas of impact relevant to the organization or activity, and may include:

- Assets and resources, including human, physical, financial, technical and information;
- Cost, both direct (including budget impacts) and indirect;
- Human resources;
- Community groups;
- Performance of activities (i.e. how well activity are performed);
- Timeliness of activities, including start-time, downstream or follow-up impacts;
- Organizational behaviour;
- Changes in SPMs' focus areas;
- Environment; and
- Intangibles.

### **Key risk categories**

Broadly, risks are categorised in the following as follows:

1. **Strategic Issues** - These are risks of a strategic nature, which include the following issues:
  - Corporate governance
  - Business continuity planning
  - Service delivery
  - Management responsibility
  - Streamlined procedures
  - Communication / Public Relations / Reputational Management
  - Organisational Structure / Change Management
2. **External risks** - These risks are caused by external factors. SPM cannot control these risks but needs to evaluate these risks and implement the appropriate actions. The category includes the following issues:
  - External stakeholders
  - Financial markets
  - Economic environment
3. **Technology risks** - Technology risk is the risk of obsolescence of infrastructure, deficiency in integration, failures/inadequacies in systems/networks and the loss of accuracy, confidentiality, availability and integrity of data. It includes the following issues:
  - Succession planning of applications
  - Disaster recovery
  - Systems development and testing
  - Software and hardware
  - Programme changes



- General access to data and programmes
4. **Financial risk** - Financial risk is the risk that the SPM will encounter difficulty in raising funds to meet commitments and the inadequate management of the finance function. It includes the following actions:
- Budget and forecasting
  - Fixed asset control
  - Internal control
  - Financial reporting
  - Misappropriation of assets and funds
5. **Human Resources** - Human resource risk is the risk of actions to/by employees. It includes the following actions:
- Recruitment
  - Remuneration
  - Training, skills and career planning
  - Performance appraisal
  - Succession planning
  - Equity
  - Acting in a way not appropriate for professionals
  - Transgression of staff rules
6. **Legal risk** - Legal risk is the risk that the SPM will be exposed to contractual obligations which have not been provided for or the inability to effect the required legal finding and action to protect the financial market. It includes the following actions:
- Contracts
  - Regulatory / Statutory Compliance
  - Litigation
  - Enforcement
  - External role players
  - Documentation availability and completeness
7. **Operational risk** - Operational risk is the risk that there is a loss as a result of failures/inadequacies in e.g., procedures, office space, personnel, electricity supply, and business relations. This includes losses as a result of errors, omissions and delay. The risk can be due to the following actions:
- Service delivery
  - Business processes
  - Regulatory trends
  - Procurement / Budgeting / Funding / Project Management
  - Fraud
  - Methods and techniques



- Standards
- Education

### **Key questions that can be used to identify and control risks**

- What, when, where, why and how risks are likely to occur, and who might be involved?
- What is the source of each risk?
- What are the consequences of each risk?
- What controls presently exist to mitigate each risk?
- To what extent are controls effective?
- What alternative, appropriate controls are available?
- What are SPM's obligations – external and internal?
- What is the need for research into specific risks?
- What is the scope of this research, and what resources are required?
- What is the reliability of the information?
- Is there scope for bench-marking with peer organizations?

### ***Identifying the potential root causes of risk events (“contributory factors”)***

Exposures reflect the potential for risks materialising. Perils or triggers cause actual events. Such triggers of events must be identified and documented. The purpose of identifying potential root causes is to give direction to risk intervention measures.

Contributory factors are the components of operational risk. Contributory factors are factors that contribute or increase the likelihood that risks could occur. In other words risks are the potential negative consequence of a contributory factor.

Contributory factors can be divided into seven major categories being:

1. People
2. Equipment
3. Business processes
4. ICT and other systems
5. Materials
6. Financial management
7. Internal and external Environment

Contributory factors have a many-to-one relationship with risk. Often more than one contributory factor could contribute to the same risk. Contributory factors also have a one-to-many relationship to risk meaning that one contributory factor could contribute to or increase the likelihood of more than one risk.

To identify contributory factors once the risk is identified, one has to ask the question "The risk is due to..? Or Why would the risk occur?"



### 3.2.4 Component 4 – Risk Assessment

Risk assessment allows an entity to consider how potential events might affect the achievement of objectives. Management assesses risk events by analysing their impact and likelihood using the scales below.

#### Impact Parameters

Severity Ranking	Continuity of Service Delivery	Safety & Environmental	Technical Complexity	Financial
<b>Critical 5</b>	Risk event will result in widespread and lengthy reduction in continuity of service delivery to customers for a period greater than 48 hours	Major environmental damage. Serious injury (permanent disability) or death of personnel or members of the public. Major negative media coverage.	Use of unproven technology for critical systems / project components. High level of technical interdependencies between system components.	Can lead to termination of Business activity
<b>Major 4</b>	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 utilised by the organisation for critical systems / project components.	Cost increase > 10%
<b>Moderate 3</b>	Reduction in service delivery or disruption for a period between 8 & 24 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%
<b>Minor 2</b>	Brief local inconvenience (work around possible). Loss of an asset with minor impact on operations	Little environmental, safety or health impacts. Limited negative media coverage.	Use of unproven or emerging technology for systems / project components.	Cost increase < 1%
<b>Insignificant 1</b>	No or minimal 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



### Likelihood Parameters

Probability Factor	Measurement Criteria	Qualification Criteria	Rating
<b>Common</b>	The risk is already occurring, or has a high likelihood of occurring more than once during the next 12 months	The risk is almost certain to occur in the current circumstances	<b>5</b>
<b>Likely</b>	The risk will easily occur, and is likely to occur at least once during the next 12 months	More than an even chance of occurring	<b>4</b>
<b>Moderate</b>	There is an above average chance of the risk occurring more than once during the next 3 years	Could occur often	<b>3</b>
<b>Unlikely</b>	The risk has a low likelihood of occurring during the next 3 years	Low likelihood, but could happen	<b>2</b>
<b>Rare</b>	The risk is unlikely to occur during the next 3 years	Not expected to happen - event would be a surprise	<b>1</b>

*Inherent risk rating = impact X likelihood*

### Residual Risk

Residual risk, is determined by taking into account the adequacy of the risk mitigating controls in place.

#### Control adequacy scales:

Adequacy Factor	Adequacy Qualification Criteria
<b>Over-controlled 90%</b>	The risk is adequately controlled and managed, but in some regards over-controlled.
<b>Adequate 80%</b>	The majority of risk exposure is adequately controlled and managed.
<b>Partially adequate 50%</b>	Some of the risk exposure appears to be adequately controlled, but there are major deficiencies.
<b>Inadequate 20%</b>	Control measures are mostly inadequate.

*Residual risk = Inherent risk – control adequacy*



The high, medium and low risk parameters can be depicted using the following risk matrix:

<b>I M P A C T</b>	<b>5</b>	<b>5</b>	<b>10</b>	<b>15</b>	<b>20</b>	<b>25</b>
	<b>4</b>	<b>4</b>	<b>8</b>	<b>12</b>	<b>16</b>	<b>20</b>
	<b>3</b>	<b>3</b>	<b>6</b>	<b>9</b>	<b>12</b>	<b>15</b>
	<b>2</b>	<b>2</b>	<b>4</b>	<b>6</b>	<b>8</b>	<b>10</b>
	<b>1</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
<b>T</b>		<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
<b>LIKELIHOOD</b>						

In order to assist in determining risk acceptability, the following thresholds will be used as guidelines;

Thresholds	Threshold Interpretation		Suggested Action	Suggested Timing
Where the result is:				
between 17 and 25		<b>RED – Unacceptable</b> High Risk	Management should take immediate action to reduce risk exposure to an acceptable level.	Immediate action required
between 8 and 16		<b>YELLOW – Cautionary</b> Medium Risk	Management should constantly monitor the risk exposure and related control adequacy.	Medium term action - within three months
between 1 and 7		<b>GREEN – Acceptable</b> Low Risk	Management should monitor risks and may consider reducing the cost of control.	Monitor – no immediate action required

Likelihood represents the possibility that a given event will occur, while impact represents its effect should it occur. Estimates of risk likelihood and impact often are determined using data from past observable events, which may provide a more objective basis than entirely subjective estimates. Internally generated data based on an entity's own experience may reflect less subjective personal bias and provide better results than data from external sources. However, even where internally generated data are a primary input, external data can be useful as a checkpoint or to enhance the analysis. Users must be cautious when using past events to make predictions about the future, as factors influencing events may change over time.

An entity's risk assessment methodology normally comprises a combination of qualitative and quantitative techniques. Management often uses qualitative assessment techniques where risks do not lend themselves to quantification or when sufficient credible data required for quantitative assessments either are not practicably available or obtaining or analyzing data are not cost-effective. Quantitative techniques typically bring more precision and are used in more complex and sophisticated activities to supplement qualitative techniques. The quantification of likelihood and impact is normally displayed in a heat map, by performing the four steps explained as part of the control environment.



Management often uses performance measures in determining the extent to which objectives are being achieved. It may be useful to use the same unit of measure when considering the potential impact of a risk to the achievement of a specified objective. Management may assess how events correlate, where sequences of events combine and interact to create significantly different probabilities or impacts. While the impact of a single event might be slight, a sequence of events might have more significant impact.

Where potential events are not directly related, management should assess them individually. Where risks are likely to occur within multiple departments/ units, management may assess and group identified events into common categories. There is usually a range of possible results associated with a potential event, and management considers them as a basis for developing a risk management strategy. Through risk assessment, management considers the positive and negative consequences of potential events, individually or by category, across the entity. Risk assessment is applied first to inherent risk – the risk to the entity in the absence of any action management might take to alter either the risk's likelihood or impact. Once risk management strategies have been developed, management then uses risk assessment techniques in determining residual risk – the risk remaining after management's action to alter the risk's likelihood or impact.

### 3.2.5 Component 5 – Risk Response Strategy

Management identifies risk response strategy options hereafter referred to more specifically as risk responses, and consider their effect on event likelihood and impact, in relation to risk tolerances, costs versus benefits, and thereafter design and implement response options.

The consideration of risk responses is integral to risk management and requires that management select a response that is expected to bring risk likelihood and impact within SPM's risk tolerance level.

After the risks have been identified and the contributing factors or root causes have been established, the control strategy should be identified for the various risk exposures. Risk responses fall within the categories of risk avoidance, active management and acceptance. The following should be used to identify the control strategies considered by management:

- Transfer through insurance cover;
- Tolerate;
- Treat/ mitigate through rigorous management practices; or
- Terminate the risk by eliminating a process, a product, or a geographical zone.

After the control strategy decision, the current controls to manage the risk in question are identified. It is necessary to assess the adequacy of these controls. This is a measure of how well management perceives the identified controls to be designed to manage the risks.

Management does this by determining the respective impact of the controls on either the inherent impact or likelihood of the specific risk. No specific rating of control adequacy is applied and this allows for management to consistently use more simplified rating mechanisms for risk and controls.



Management should recognize that some level of residual risk will always exist, not only because resources are limited, but also because of inherent future uncertainty and limitations inherent in all activities.

### 3.2.6 Component 6 – Information and Communication

Pertinent information – both from internal and external sources, financial or non-financial – must be identified, captured and communicated in a form and timeframe that enable personnel to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across and up the organisation, as well as the exchange of relevant information with external parties, such as customers, suppliers, regulators and shareholders.

Information is needed at all levels of an entity to identify, assess and respond to risks, and to otherwise run the entity and achieve its objectives. An array of information is used, relevant to one or more objectives categories. Information comes from many sources – internal and external, and in quantitative and qualitative forms – and allows risk management responses to changing conditions in real time.

The challenge for management is to process and refine large volumes of data into relevant and actionable information. This challenge is met by establishing an information systems infrastructure to source, capture, process, analyse and report relevant information. These information systems – usually computerized but also involving manual inputs or interfaces – often are viewed in the context of processing internally generated data relating to transactions.

Information systems have long been designed and used to support organisational strategy. To support effective risk management, an entity captures and uses historical and current data. Historical data allow the entity to track actual performance against targets, plans and expectations. It provides insights into how the entity performed under varying conditions, allowing management to identify correlations and trends and to forecast future performance. Historical data also can provide early warnings of potential events that warrant management attention.

Present or current state data allow an entity to assess its risks at a specific point in time and remain within established risk tolerances. Current state data allow management to take a real-time view of existing risks inherent in a process, function or unit and to identify variations from expectations. This provides a view of SPM's risk profile, enabling management to alter activities as necessary to fit in with the acceptable level of risk

Information is a basis for communication, which must meet the expectations of groups and individuals, enabling them to effectively carry out their responsibilities. Among the most critical communications channels is that between top management and the executive authority.

Management must keep the executive authority up-to-date on performance, developments, risks and the functioning of risk management, and other relevant events and issues. The more effective the communication, the more successful the executive authority will be in carrying out its oversight responsibilities, in acting as a sounding executive authority on critical issues and in providing advice, counsel and direction. By the same token, the executive authority should communicate to management what information it needs and provide feedback and direction.



Management provides specific and directed communication addressing behavioural expectations and the responsibilities of personnel. This includes a clear statement of SPM's risk management philosophy and approach and delegation of authority. Communication about processes and procedures should align with, and underpin, the desired risk culture. In addition, communication should be appropriately "framed" – the presentation of information can significantly affect how it is interpreted and how the associated risks or opportunities are viewed.

Communication should raise awareness about the importance and relevance of effective risk management, communicate SPM's risk tolerance levels, implement and support a common risk language, and advise personnel of their roles and responsibilities in effecting and supporting the process of risk management. Communication channels also should ensure personnel can communicate risk-based information across units, processes or functional silos. In most cases, normal reporting lines in an entity are the appropriate channels of communication. In some circumstances, however, separate lines of communication are needed to serve as a fail-safe mechanism in case normal channels are inoperative. Whatever channels of communication are used, it is imperative that personnel understand that there will be no reprisals for reporting relevant information.

External communications channels can provide highly significant input on the design or quality of products or services. Management considers how its risk tolerance aligns with those of its customers, suppliers and partners, ensuring that it does not inadvertently take on too much risk through its department interactions.

### **3.2.7 Component 7 – Control Activities**

Risk responses serve to focus attention on control activities needed to help ensure that the risk responses are carried out properly and in a timely manner. Control activities are part of the process by which an entity strives to achieve its business objectives.

Control activities are the policies and procedures that help ensure risk management strategies are properly executed. They occur throughout the entity, at all levels and in all functions. Internal control is an integral part of risk management.

Control procedures relate to the actual policies and procedures in addition to the control environment that management has established to achieve SPM's objectives. Policies and procedures help create boundaries and parameters to authority and responsibility, and also provide some scope of organisational precedent for action.

### **3.2.8 Component 8 – Monitoring**

Risk management should be regularly monitored – a process that assesses both the presence and functioning of its components and the quality of their performance over time. Monitoring can be done in two ways: through ongoing activities or separate evaluations. This will ensure that risk management continues to be applied at all levels and across the entity.

Ongoing monitoring is built into the normal, recurring operating activities of an entity, is performed on a real-time basis and reacts dynamically to changing conditions and is ingrained in the entity. As a result, it is more effective than separate evaluations. Since separate evaluations take place after the



fact, problems often will be identified more quickly by ongoing monitoring routines. Many entities with sound ongoing monitoring activities nonetheless conduct separate evaluations of risk management.

The frequency of separate evaluations is a matter of management's judgment. In making that determination, consideration is given to the nature and degree of changes, from both internal and external events, and their associated risks, the competence and experience of the personnel implementing risk management strategies and related controls and the results of the ongoing monitoring. Usually, some combination of ongoing monitoring and separate evaluations will ensure that risk management maintains its effectiveness over time.

The extent of documentation of an entity's risk management varies with the entity's size, complexity and similar factors. The fact that elements of risk management are not documented does not mean that they are not effective or that they cannot be evaluated. However, an appropriate level of documentation usually makes monitoring more effective and efficient. Where management intends to make a statement to external parties regarding risk management effectiveness, it should consider developing and retaining documentation to support the statement.

All risk management deficiencies that affect an entity's ability to develop and implement its strategy and to achieve its established objectives should be reported to those positioned to take necessary action. The nature of matters to be communicated will vary depending on individuals' authority to deal with circumstances that arise and on the oversight activities of superiors. The term "deficiency" refers to a condition within the risk management process worthy of attention. A deficiency, therefore, may represent a perceived, potential or real shortcoming, or an opportunity to strengthen the process to increase the likelihood that the entity's objectives will be achieved. Information generated in the course of operating activities usually is reported through normal channels. Alternative communications channels also should exist for reporting sensitive information such as illegal or improper acts, fraud, corruption and theft.

Providing relevant information on risk management deficiencies to the right party is critical. Protocols should be established to identify what information is needed at a particular level for effective decision making. Such protocols reflect the general rule that a manager should receive information that affects actions or behaviour of personnel under his or her responsibility, as well as information needed to achieve specific objectives.

### ***Key risk indicators***

Key risk indicators are intended to assist management to monitor risks. Key risk indicators have two focal points i.e. the inherent risk itself as well as losses, incidents and variances. Each key risk should have a key risk indicator to serve as a risk warning mechanism.

Each business unit is responsible for defining, monitoring and reporting on key risk indicators for all key risks identified.

### ***Risk tolerance limits***

Risk tolerances are the acceptable levels of variation relative to the achievement of objectives. Risk tolerances can be measured, and often are best measured in the same units as the related objectives. Performance measures are aligned to help ensure that actual results will be within the acceptable risk



tolerances. In setting risk tolerances, management considers the relative importance of the related objectives and aligns risk tolerances with risk appetite. Operating within risk tolerances provides management greater assurance that the entity remains within its risk appetite and, in turn, provides a higher degree of comfort that the entity will achieve its objectives.

Each group company is responsible for defining its own risk tolerance limits for all key risks identified.

### ***Incident reporting***

This is an internal management function and will form part of the Enterprise Risk Management process. Incident reports should incorporate:

- Incidents of non-compliance to approved standards (whether losses were incurred or not); and
- Losses arising from particular incidents.

The destination of incident reports will be determined by the nature of the potential or actual loss. Incidents and losses that originate from risks contained in the key risk registers must always be elevated to higher levels of management with risk-related variance reports being incorporated into routine management reporting processes.

### ***Performance measurement***

Management's performance with regards to Enterprise Risk Management will be measured and monitored through the following performance management activities:

- Monitoring of progress made by management with the implementation of the Enterprise Risk Management methodology;
- Monitoring of key risk indicators;
- Monitoring of loss and incident data;
- Management's progress made with risk mitigation action plans; and
- An annual quality assurance review of Enterprise Risk Management performance.

## **3.3 Governance requirements**

### **3.3.1 Establish an organisational framework of assurance for key risks and controls**

A framework of assurance must be developed for SPM's risks. Key players in the organisation will combine to provide assurance that risks are being appropriately managed. This combined approach to assurance normally involves management, internal auditors and external auditors working together through an integration process coordinated by the Audit and Risk Committee. Other experts must be chosen to provide assurance regarding specialised categories of risk, such as environmental management and capital market risks. The assurance framework must be formalised and must incorporate appropriate reporting processes.



### **3.3.2 Internal audit provides assurance on risk management processes**

Internal audit must examine the techniques used to identify risk. The categories and the scope of risk assessments should be considered. The methodologies used to extract risk information must be reviewed. Monitoring processes should be wholly aligned with the results of risk assessments. The internal audit function should particularly seek evidence that the processes of risk identification are dynamic and continuous, rather than attempt to comply with governance expectations. The effectiveness of Enterprise Risk Management processes should be subjected to an audit on an annual basis.

### **3.3.3 The outputs of risk assessments are used to direct internal audit plans**

Internal audit plans depend greatly on the outputs of risk assessments. Risks identified during risk assessments must be incorporated into internal audit plans, in addition to management and Audit and Risk Committee priorities. The risk assessment process is useful for internal audit staff because it provides the necessary priorities regarding risk as opposed to using standardised audit sheets. The audit activities will focus on adherence to controls for the key risks that have been identified. In addition, internal audit staff may direct management towards the need for better controls around key risks.

### **3.3.4 Internal audit provides assurance on quality and reliability of risk information**

The internal audit function plays a key role in co-ordinating the key players in the risk management process to provide assurance to stakeholders. Internal audit is not normally the only provider of assurance. The function does, however, have an important role in evaluating the effectiveness of control systems. The process of assurance must also involve management, the external auditors, regulators and subject specialists.

### **3.3.5 Safety, health and environment**

A formal safety management programme is essential for SPM's business. The risks will vary according to the entity, but the principles of risk management will always apply, i.e. risk identification, risk assessment, formal action plans for mitigation, monitoring, reporting and assurance. The scope of SPM's safety management programme should include administrative aspects, safety awareness and training, health, hygiene, electrical safety, physical safety, micro-environmental exposures and legislative requirements.

### **3.3.6 Business Continuity Management**

It is expected that SPM will have a Business Continuity Management Plan in place, which will be revised and tested annually. The results of such testing and simulations should be reported to the Audit and Risk Committee.



### 3.3.7 Fraud Prevention and Anti-corruption Plan

SPM is responsible for developing and implementing its own Fraud Prevention and Anti Corruption Plan. Confidential reporting of potential breaches and actual investigations should be reported to the MM and the Audit and Risk Management Committee.

**Prepared by:**

**Approved by:**

---

W.L. Wiese  
**Risk Officer**

---

G.H. Akharwaray  
**Municipal Manager**

---

Date

---

Date

