

RISK MANAGEMENT STRATEGY 2013/14

TIP- OFF ANONYMOUS

FRAUD HOTLINE

TEL: 0800 004 004

FAX 0866 614 1027

E-MAIL: Merafong@thehotline.co.za

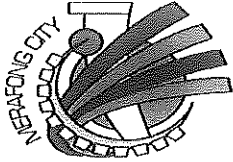
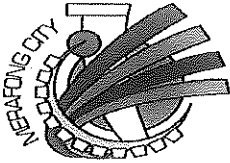


TABLE OF CONTENTS

Contents

1. RISK MANAGEMENT OBJECTIVES.....	3
2. LEGAL MANDATE.....	4
3. BENEFITS OF RISK MANAGEMENT.....	5
4. RISK MANAGEMENT STRUCTURES AND RESPONSIBILITIES.....	5
5. RISK MANAGEMENT PROCESS.....	8
6. RISK MANAGEMENT REPORTING.....	11
7. REVIEW.....	12
Appendices.....	13
Appendix A: Definitions and CRITERIA FOR RISK evaluation.....	13
Appendix B - Assessment tables.....	16
Appendix C: Risk Category Model.....	18



1. RISK MANAGEMENT OBJECTIVES

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

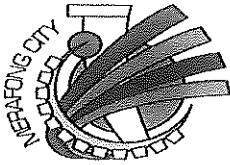
- Ensure Compliance with the Municipal Finance Management Act and its accompanying Treasury Regulations.
- Safeguard the company's assets and investments.
- Support achievement of strategic objectives.
- Behave responsibly towards all stakeholders.
- Ensure service delivery to all stakeholders.

Effective risk management is therefore a key tool to ensure that MCLM achieves its objectives. What is implicit in the objectives is that:

- 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.
- 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.

Risk management has been defined as "a continuous, proactive and systematic process, affected by MCLM's Council, Executive Mayor, Municipal Manager, senior management and other personnel, applied in strategic planning and across the company, designed to identify potential events that may affect the municipality , and manage risks to be within its risk tolerance, to provide reasonable assurance regarding the achievement of its strategic objectives."

A major component of risk management is the establishment of a fraud prevention plan. Managing the risk of fraud and corruption entails the development, implementation, and maintenance of cost effective internal controls.



2. LEGAL MANDATE

2.1 Municipal Finance Management Act: S95 (c)

The accounting officer of a municipality –

must ensure that the municipality has and maintains

- (i) effective, efficient and transparent systems of financial and risk management and internal control;
- (ii) a system of internal audit;
- (iii) an appropriate procurement and provisioning system which is fair, equitable, transparent, competitive and cost-effective;
- (iv) a system for properly evaluating all major capital projects prior to a final decision on the project;

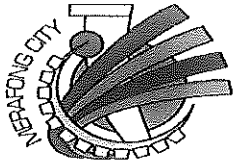
2.2 King III Report on Corporate Governance.

- (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 roles and responsibilities for the implementation of a Risk Management strategy can be summarised as follows:

- The Municipal Manager must ensure that a risk assessment is conducted regularly to identify emerging risks for the institution.
- 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.
- 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.

The King report on Corporate Governance also reflects on risk management as an integral part of strategic and operational activities.



3. BENEFITS OF RISK MANAGEMENT

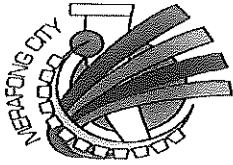
The risk management process is being implemented by MCLM as it will assist with the achievement of objectives. The benefits of risk management are:

- **Organisational alignment:** The risk management process is designed to compliment effective strategic and operational planning. However, as the risk management approach is objective driven it will assist in ensuring that management and staff understand 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.
- **Improved ability to manage risks:** By formally identifying and evaluating risks we will improve our understanding of the risks which need to be managed. Furthermore, we will analyse and understand the causes of risks to ensure our internal controls manage these causes.
- **Improved ability to achieve objectives:** By proactively identifying risks a company will have a better understanding of risks and be more anticipatory and therefore able to achieve its objectives with greater certainty.
- **Improved ability to seize opportunities:** By understanding our risk profiles, the risk management process will enable us to seize and execute new opportunities successfully.
- **Cost Effective Internal Controls:** The risk management process will ensure that our system of internal control is cost effective. Areas of over control should be identified and removed.
- **Sustainability:** The risk management process is a means to educate all our 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 MCLM.

4. RISK MANAGEMENT STRUCTURES AND RESPONSIBILITIES

Municipal Manager (MM)

The Municipal Manager is ultimately responsible for and should assume "ownership" of risk management. More than any other individual, the MM sets the "tone at the top" that affects integrity and ethics and other factors of the control environment. This duty is fulfilled by providing leadership and direction to senior managers and reviewing the way they manage the process.



The MM, through the Council is ultimately responsible for ensuring that a risk management process is implemented throughout MCLM. Management is accountable to the MM, which provides governance, guidance and oversight. By selecting management, the MM has a major role in defining what it expects in integrity and ethical values and can confirm its expectations through oversight activities. Similarly, by reserving authority in certain key decisions, the MM plays a role in setting strategy, formulating high-level objectives and broad-based resource allocation. The MM provides oversight with regard to risk management by:

- Knowing the extent to which management has established effective risk management in the company;
- Being aware of and concurring with the risk tolerance;
- Reviewing risks and considering it against the risk tolerance; and
- Being aware of the most significant risks and whether management is responding appropriately.

Management

Management is accountable to the MM for designing, implementing and monitoring the process of risk management and integrating it into the day-to-day activities.

Senior managers assign responsibility for establishment of more specific risk management policies and procedures to personnel responsible for individual units' functions. Also significant are leaders of staff functions such as compliance, finance, human resources and information technology, whose monitoring and control activities cut across, as well as up and down, the operating and other business units.

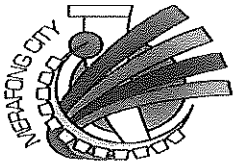
Audit Committee

The Audit Committee will function as a monitoring and oversight body to ensure that risk management is embedded within MCLM.

Risk Management Committee

Risk management committee, comprising senior management of all divisions, will be established to ensure that risk is being managed on a day-to-day basis and will provide reports on the status of significant risks to the Audit Committee.

The Risk Committee will assist the MM in discharging its risk management responsibilities. The composition and Terms of Reference of this Committee is set out in a separate document.



Manager: Risk Management/Chief Risk Officer

To assist management in their risk management duties a risk management function will be set up under a risk officer. The risk management function or risk officer will be:

- Responsible for educating management and staff in the risk management process.
- Responsible for creating an awareness of risk and assisting management in ensuring that there is a culture of control.
- Available to assist in the risk profiling exercises.
- Responsible for consolidating risk reports for the Audit Committee.

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

A Risk Officer works with other managers in establishing and maintaining effective risk management in their areas of responsibility. The Risk Officer also may have responsibility for monitoring progress and for assisting other managers in reporting relevant risk information up, down and across the MCLM, and may be a member of an internal risk management committee.

Employees

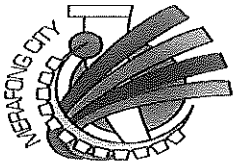
Risk Management is the responsibility of everyone in the organisation and therefore it should be an explicit or implicit part of everyone's job description. Virtually all personnel produce information used in risk management or take other actions needed to manage risks. Employees are responsible for communicating risks such as problems in operations, non-compliance with the code of conduct, other policy violations or illegal actions.

A number of external parties often contribute to achievement of MCLM objectives. Others providing information to the MCLM useful in effecting risk management are regulators, customers, suppliers, and the media. External parties, however, are not responsible for the MCLM's risk management.

Assurance Providers

Internal audit and other assurance providers will provide assurance to management and the Audit Committee that adequate and effective risk management and control processes are in place throughout the company.

External auditors bring an independent and objective view, contributing directly through the financial statement audit and internal control examinations, and indirectly by providing



additional information useful to management and the executive authority in carrying out their responsibilities.

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 is approved by the audit committee. They may assist both management and the Council or Audit Committee by monitoring, examining, evaluating, reporting on and recommending improvements to the adequacy and effectiveness of management's risk management processes. Such request should however be routed through the audit committee to ensure that such involvement does not effect the completion of the approved audit plan.

5. RISK MANAGEMENT PROCESS

In implementing our risk management policy, we undertake the following:

- To define and implement a context for risk management by:
 - Creating an appropriate control environment of values, discipline and structure.
 - Developing a centrally co-ordinated risk framework and management process to ensure consistency. This will include the development of a Fraud Prevention Plan.
 - Ensuring that risk management is not one event, but a series of continuous actions that permeate our activities.
 - Defining the responsibility structure for risk management.
 - Develop a clear and unambiguous understanding of our strategic objectives and purpose.
 - Continually evaluating and reviewing the internal and external environment for risks that may effect the achievement of our strategic objectives.
 - Continually reviewing our risk tolerance as our internal and external environment changes.
- To implement the following continuous risk management process :
 - An annual review of the most significant risks facing MCLM.
 - Assessment and evaluation of the inherent impact and likelihood of risk occurring.

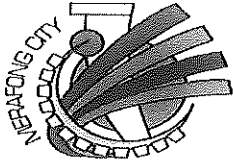


- Determination of the MCLM's response to the risk – Take, Manage, Transfer (insure) or Avoid. Cost benefit as well as service delivery considerations will be a factor in deciding on the most suitable response.
- Where the response is to manage or transfer the risk, we will examine existing procedures and controls in place to manage the risk to an acceptable level.
- Re-evaluation of the risk after taking controls into account, to obtain the residual risk/ exposure.
- Consideration of any enhancements to control that may be required to reduce residual exposure to an acceptable level.
- Continual monitoring of the status of risks and develop a process for appropriate action if that status changes.
- Report to senior management and the audit committee on an ongoing basis regarding the results and status of risk management.
- Maintaining an awareness of risk and risk management process.

The risk framework will consider the following risk categories:

- Strategic,
- Governance,
- Service Delivery,
- Culture,
- Organisational structure,
- Reputation,
- Financial,
- Procurement,
- Budgeting,
- Communication,
- Legal,
- Compliance,
- Fraud,
- Technology,
- Human Resources,

Our risk management strategy will be reviewed on an annual basis to ensure that it remains appropriate and that the latest best practice risk management has been adopted where appropriate.



In order to achieve the required strategic objectives, MCLM needs to take certain risks. Senior management is responsible for understanding the level of risk which has been taken to achieve objectives, as well as the process in place to mitigate these risks. Based on the need to balance the achievement of performance against the need to protect its stakeholders, MCLM 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 process.

The risk management process consists of the following key stages:

1 Risk Profiling

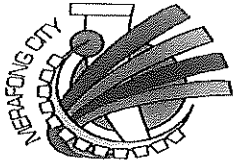
- **Determination of objectives:** The objectives should be identified along with the key performance indicators to measure the achievement of these objectives.
- **Identification of risks:** The risks which can prevent the achievement of the objectives will be identified. Identification of risks will 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**.
- **Risk Evaluation:** The impact and likelihood of risks, pre and post considering the current systems, controls, processes and people in place will be assessed using the criteria in **Appendix C**.
- **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.

2 Review of Internal Controls

- **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 are:
Accept: Each risk can be accepted. This is normally the case for low impact risks with a low likelihood of occurrence.

Avoid: 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.

Manage: 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 insurance company. Note the transfer of risks normally occurs for risks with a high impact but a low likelihood of occurrence.

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:

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 do 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.

3. Risk and Control Monitoring

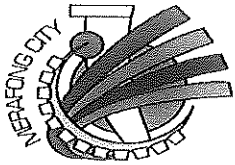
- **Key Risk Indicators:** For each of the risks in the profiles, where appropriate, management will identify the key risk indicators which should be monitored to determine if the risk is likely to materialise. These key risks indicators will compliment our key performance indicators and will be included in our management reporting.
- **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.
- **Reassessment of risks:** Some risks, by their nature, need to be re-evaluated 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. 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 our requirements and risk management practices evolve. Basic protocols have been set out below.

Risk information that must be reported includes:

- Key risks – including the impact and likelihood pre control, controls in place to manage the risk and residual risk post control consideration.



- Any material changes to the risk profile.
- Summaries of significant control breakdowns/ losses.
- Breaches of controls or legal requirements
- The results of assurance work to date.

Escalation procedures should be in place to ensure that appropriate material risk issues are reported timeously to the appropriate person.

To assist management in maintaining and monitoring their risk profiles, as well as for providing reports for the Risk and Audit Committees, a decision has been taken to use risk management software to support the risk management process.

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.

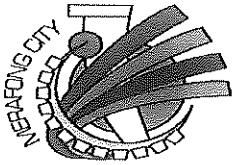
However, the MM recognises that there also needs to be a sound system of risk management and internal control in place at a process level. Management is accountable, as above, for ensuring that this is achieved.

However, it is not practical or cost effective to implement the above risk management process to all our processes throughout MCLM. As such, at a process level the Municipal Manager 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 Audit Committee.

7. REVIEW

The terms of reference will be reviewed as and when new and relevant changes require to be effected to the policy.



Appendices

Appendix A: Definitions and CRITERIA FOR RISK evaluation

KEY DEFINITIONS.

Risk

The threat that an event or action will adversely affect the MCLM ability to achieve its business objectives and successfully execute strategy.

Strategic Risk

- Risks attached to the decision-making, operations and actions at the strategic management level.
- Strategic risk relates to the consequences that occur when the environment has an unattractive or adverse impact.

Operational Risk

- Risk of loss due to deficiencies or failures in operational processes, people, information systems, management failures and external events.
- These risks include legal risk but exclude strategic and reputational risks.

Cause

- Underlying factors / causes / weaknesses that would give rise to a risk(s).

Consequence

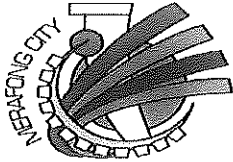
The consequence is the impact to MCLM if the risk materializes.

Controls

The means used to manage a risk. In particular, a policy, procedure, device, system, communication or other action that acts to limit uncertainty in the achievement of business objectives and/or to ensure compliance with the law.

Risk Assessment Criteria

- Inherent Risk= Probability x Impact
- Residual Risk = Inherent Risk x (1- Control Effectiveness)



Lists of Identified Institutional Risks

The risks facing MCLM will be confirmed and clearly documented. It is necessary to identify all the potential risks and threats relating to business processes, assets and strategy which are possible problems and situations that may hinder the achievement of the objectives. For each risk identified the following must be assessed:

1 The severity (Impact)

This is the potential magnitude of the impact on your objectives, should the risk actually occur. This must be assessed on the basis that management has no specific controls in place to address the risk, i.e. without any controls in place, what will the impact of this risk be on your company?

2 The probability of occurrence (Likelihood)

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

Scales of impact and probability will be determined and will be explained during the workshop, and applied consistently throughout the process. The relevant categories, with explanations, are set out in this document in Appendix C.

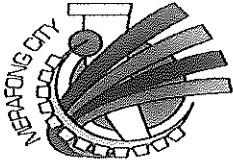
Inherent risk

Inherent risk is the product of the potential impact of a risk and the probability of that risk occurring. The value for inherent risk assists management to establish relativity between all the risks identified for the process. This indicator may be used to assign the level of management resources required to control the relevant risks.

Risk Mitigation (Controls, Insurance, etc)

These consist of processes, procedures, equipment or other actions implemented by management to increase the likelihood that MCLM objectives will be achieved. Each risk may be mitigated by one or multiple mechanisms in order to effectively reduce the risk to a level that is acceptable to management and other stakeholders. Generally, the "four T" principle is applied, i.e.

- Transfer the risk,
- Treat the risk,
- Tolerate the risk,
- Terminate the risk.



Control Assessment

Having established which controls are in place to manage the risk in question, it is necessary to assess the effectiveness of the controls. This is a measure of how well management perceives the identified controls to be working and effectively managing the risks. A standard table that classifies controls into 5 different levels of perceived effectiveness is used, namely:

Very good	Good	Satisfactory
Weak	Unsatisfactory	

The relevant categories, with explanations, are set out in **Appendix C**.

Residual Risk Status and Ranking

This is the level of risk that the MCLM is actually exposed to, taking into account the potential impact of the risk, the probability of the risk occurring and the related controls which exist to manage that risk.

This information assists decision makers in assessing the acceptability of the residual risk exposure and in deciding whether further management action is required to reduce the risk exposure.

Risk Treatment (Management Action)

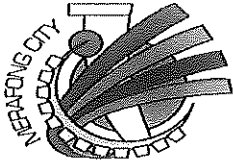
Based on the value of the residual risk exposure, management will decide whether they are willing to accept the identified level of residual risk exposure.

If the residual risk is considered to be too high, then an action plan should be prepared to reduce the risk to a level that is more acceptable to management and stakeholders.

Management actions may include the re-examination of the control design for the business objective identified earlier in the risk management process.

The action plans must clearly identify:

- The required actions;
- The person(s) responsible for implementing the action, and
- The applicable completion dates/timeframes.



Appendix B - Assessment tables

Qualitative Assessment of Potential Impact

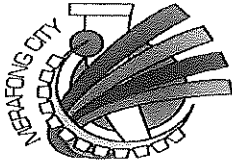
The following table is to be used to assist the participants in quantifying the potential impact that a risk exposure may have on MCLM.

Rate	Impact	Description
5	Catastrophic	Loss of ability to sustain ongoing operations. A situation that would cause our business to cease operations.
4	Major	Significant impact on achievement of strategic objectives and targets relating to MCLM.
3	Moderate	Disruption of normal operations with a limited effect on achievement of strategic objectives or targets relating to MCLM.
2	Minor	No material impact on achievement of the MCLM strategy or objectives.
1	Insignificant	Negligible impact.

Qualitative Assessment of Probability of Occurrence

The table below is to be used to assist participants in quantifying the probability of a specific risk occurring in the business.

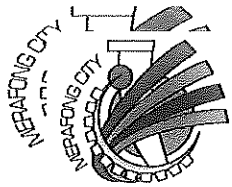
Rate	Probability Factor	Qualification Criteria
5	Certain	Has or will occur
4	Likely	More than an even chance of occurring
3	Moderate	Could occur quite often
2	Unlikely	Small likelihood but could happen
1	Rare	Not expected to happen - Event would be a surprise



Qualitative Assessment of Control

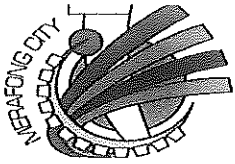
The table below is to be used to assist participants in quantifying the effectiveness of controls to mitigate or reduce the impact of specific risks on the business.

Rate	Effectiveness Factor	Qualification Criteria
5	Very Good	Risk exposure is effectively controlled and managed
4	Good	Majority of risk exposure is effectively controlled and managed
3	Satisfactory	There is room for some improvement
2	Weak	Some of the risk exposure appears to be controlled, but there are major deficiencies
1	Unsatisfactory	Control measures are ineffective

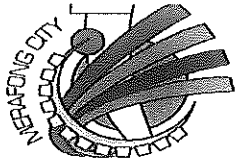


Appendix C: Risk Category Model

Risk type	Broad definition	Examples of key risks
Strategic	The risk that strategic intent and direction cannot be sustained and/or objectives cannot be achieved	<ul style="list-style-type: none"> • Inappropriate strategy • Incorrect implementation of strategic objectives. • Wrong strategic decision taken • Lack of leadership • Inadequate succession planning resulting in inability to achieve objectives
Governance	The structures and processes in place to ensure good governance in the organisation	<ul style="list-style-type: none"> • Lack of strategy and objectives • Lack of or inappropriate delegation of authority • Lack of or inadequate policies and procedures • Lack of or inappropriate communication and reporting structures • Nepotism
Service Delivery	The strategic objective and mission of MCLM to ensure that it meets the objectives and service delivery targets.	<ul style="list-style-type: none"> • Poor service delivery • Inefficient service delivery..
Culture	The alignment of ethics and values in MCLM	<ul style="list-style-type: none"> • Poor or inconsistent ethics and values. • Different beliefs and values impacting goal alignment. • Different beliefs and values impacting acceptance of change and integration
Organisational Structure	The risk that organisational structure is not suited to achievement of objectives	<ul style="list-style-type: none"> • Inappropriate organisational structure • Strategy change without appropriate organisational structure change
Reputation	The risk that the actions or inaction harms the reputation of MCLM	<ul style="list-style-type: none"> • Damage to brand due to adverse public event • Damage to reputation due to release of inaccurate information
Finance	The risk of financial loss or incorrect financial decisions being made.	<ul style="list-style-type: none"> • Incomplete, inaccurate or unreliable financial information. • Inadequate financial reporting for decision making • Lack of or inappropriate finance policies and procedures. • Financial loss/ loss of assets
Procurement	The risk of unauthorised or inappropriate procurement	<ul style="list-style-type: none"> • Lack of procurement policies and procedures • Unauthorised expenditure



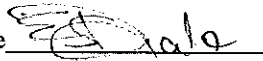
Budgeting	The risk that the budgeting process is inadequate or inappropriate to achieve objectives.	<ul style="list-style-type: none"> • Inadequate funding • Inaccurate budgeting and planning.
Communication	Inappropriate or ineffective communication.	<ul style="list-style-type: none"> • Lack of communication structures or processes. • Inappropriate or inadequate reporting
Legal	<ul style="list-style-type: none"> ▪ the risk that MCLM will be exposed to contractual obligations which have not been provided for ▪ unwillingness of a counterparty to discharge contractual obligations 	<ul style="list-style-type: none"> • Incorrect legal advice given on the law or contractual interpretation
Compliance	Is the risk of not complying with policies and procedures/ laws and regulations	<ul style="list-style-type: none"> • Failure to comply, detect or report non compliance with external (e.g. statutes, common law and client mandates) and internal requirements (e.g. approval framework)
Fraud	The risk of fraud, corruption of maladministration	<ul style="list-style-type: none"> • Loss of finance or assets due to fraud, corruption or maladministration. •
Technology	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	<ul style="list-style-type: none"> • Inadequate procedures to prevent, detect and follow-up on access violations (including data, application, firewall and internet) • Inaccurate or unreliable information due to system problem/failure. • Non compliance with the information security policy, e.g. change control, e-mail Policy, anti malicious code, etc. • Inadequate procedures to develop, maintain and test the BCP / Disaster Recovery plan (including telecommunications, data backup)
Human Resource	<p>The risk of ineffective or inefficient HR practices and infrastructure</p> <p>The risk that employees are unable to achieve objectives.</p>	<ul style="list-style-type: none"> • Inappropriate alignment of staff and culture to strategy and values • Exposure to loss of key employees • Inadequate measurement, and management of staff performance and development • Lack of or inappropriate employee training. • Poor recruitment decisions • Inability of employee to perform their functions adequately and effectively
Employee Value	The risk that employees are not valued	<ul style="list-style-type: none"> • Lack of employee motivation • Poor productivity of employees • Employees not adequately compensated • Poor retention of employees



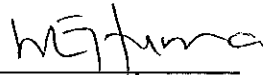
Security	The risk that human resources or physical assets are not appropriately safeguarded	<ul style="list-style-type: none">• Loss or theft of assets• Loss of or endangerment of human life
-----------------	--	---

10. APPROVAL AND ADOPTION

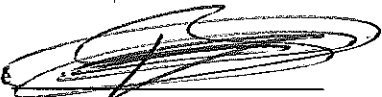
COMPILED BY
E SEGAKWENG-DIALE
MANAGER RISK MANAGEMENT

Signature 
Date 29/08/2014

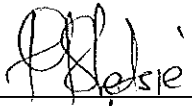
REVIEWED BY
RISK MANAGEMENT COMMITTEE
Adv. WE HUMA (Chairperson)

Signature 
Date 05/02/2015

SECONDED BY
LR THIBINI
ACTING MUNICIPAL MANAGER

Signature 
Date 10/04/2015

APPROVED BY
CLLR S. M MOGALE LETSIE
EXECUTIVE MAYOR

Signature 
Date 23/11/2015