MADIBENG LOCAL MUNICIPALITY

Risk Management Framework, Strategy, Policy & Standard Operating Procedures 2020/2021

53 van Velden Street, Brits, 0250

Table of Contents

Document Ref. No.:	ERM/p1001
Resolution no.:	
Authors / developed by:	ERM Manager: Yvonne Mothibi
Revision / Last Updated:	2020/2021
Applicability	Madibeng Local Municipality main offices and its satellite offices
Effective Date	
Approved by	Council

Abbreviations and definitions of general terms

In this policy unless otherwise indicated or stated the following terms and abbreviations have the meanings assigned to them as follows.

"**MFMA**" shall mean Municipal Finance Management Act 56 of 2003.

"**MSA**" shall mean Municipal Systems Act 32 of 2000.

"**RMC**" shall mean the Risk Management Committee.

"**CRO**" shall mean the Chief Risk Officer.

"**Accounting Officer**" shall mean the Municipal Manager.

"**Municipality**" or"**MLM**"shall mean Madibeng Local Municipality.

"**Accounting Authority**" shall mean Council.

"**COSO Framework**" refers to the framework by Committee of Sponsoring Organisations of the Treadway Commission.

RISK MANAGEMENT FRAMEWORK

Enterprise Risk Management Environment

In order to ensure the inclusion of all factors impacting on Risk Management within the Municipality, it is important to identify the environment within which the municipality operates. As with most municipal disciplines, the risk management environment has altered substantially and requires a complete review of the current policies, practices and assumptions.

Risk Environment

- Natural Disasters
- Accidents
- Injuries
- Service Failures
- Aging Infrastructure
- Loss of Skill
- Economy
- Repairs and maintenance

Council

Audit Committe

Risk Committee

Accounting Officer

- Governance
- Legislation
- Other Spheres
- Local Economic Development
- Grants

CRO Directors Line Management Internal Audit	Framework, Strategy & Policy Implementation Plan Standard Operating Procedure
Workers Community	Risks and Opportunities (Risk Register)

External Assurance Providers

Auditor General

RISK STRATEGY

Factors within the municipal environment that impact directly on how the municipality will address risk management are:

1. Legislation and guidelines
2. Unfunded Mandates
3. The entire community including residents, businesses, farmers, government, visitors, ward committees, staff, etc.
4. National Government, North West Provincial Government and Bojanala District Municipality
5. Service Providers e.g. Eskom
6. Global and local economy
7. Assets (infrastructure, land and buildings)
8. Affordability (Budget)
9. Skill Levels (Staff & Service Providers)
10. Systems (Enterprise Risk Management architecture such as information Technology, Fleet Management, debt Collection, Procurement, etc)
11. King Code

Some of these factors are compulsory, others meet good governance or best practice principles and some are inherent to Madibeng Municipality. Although Municipalities are of a similar nature and are responsible to deliver the same basic services they vary due to unique geographical, social and political nuances and cannot be addressed in the same manner across the whole of South Africa.

Enterprise Risk Management Architecture

Any successful implementation of Enterprise Risk Management is dependent on a structure that considers various interrelated and inter-dependent components. The National Treasury Public Sector Framework (National Treasury, 2010) adopts the following architecture, consisting of;

- Process framework
- Drivers
- Enablers
- Implementers
- Support
- Tools and Technology
- Assurance Providers
- Oversight framework
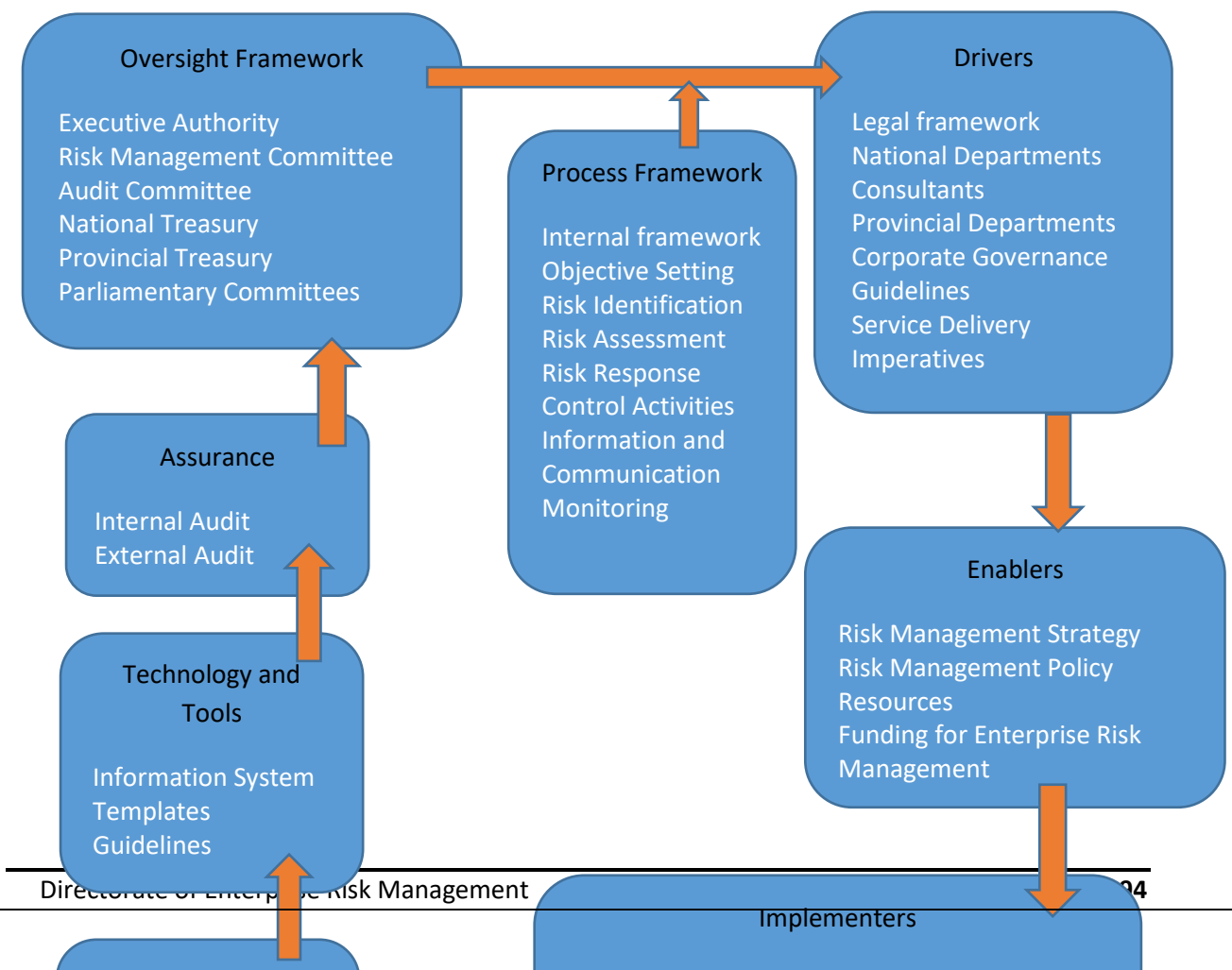
> **Differences to National Treasury Model**
>
> To bring it in line with Madibeng Municipality's current practice and structure, the Enterprise Risk Management has been amended slightly to accommodate the following changes:
>
> Removing provincial public entity from the "Drivers"
>
> Adding PMS, IA and ERM under "Implementers"

The enterprise risk management architecture is depicted graphically below:

ENTERPRISE RISK MANAGEMENT ARCHITECTURE

Oversight Framework
Executive Authority
Risk Management Committee
Audit Committee
National Treasury
Provincial Treasury
Parliamentary Committees

Drivers
Legal framework
National Departments
Consultants
Provincial Departments
Corporate Governance
Guidelines
Service Delivery
Imperatives

Process Framework
Internal framework
Objective Setting
Risk Identification
Risk Assessment
Risk Response
Control Activities
Information and
Communication
Monitoring

Assurance
Internal Audit
External Audit

Technology and Tools
Information System
Templates
Guidelines

Enablers
Risk Management Strategy
Risk Management Policy
Resources
Funding for Enterprise Risk Management

Implementers

Legislative Environment

The Municipal Finance Management Act no.56 of 2003 (MFMA) defines the Municipal Manager as the Accounting Officer. Section 62 of the MFMA requires the Accounting Officer to take all reasonable steps to ensure that the municipality has and maintains effective, efficient and transparent system of financial and risk management and internal control and of internal audit, as well as the effective, efficient and economical use of the resources of the municipality. The purpose of the risk management policy is to enable the municipality to comply with the requirements as set out in the legislation.

General Financial Management Functions

62. (1) The Accounting Officer of a municipality is responsible for managing the financial administration of the municipality, and must for this purpose take reasonable steps to ensure –

(c) That the municipality has and maintains effective, efficient and transparent systems –

(i) Of financial and risk management and internal control

The Constitution confers to the following arears of responsibility on local municipalities:

152. Objects of local government

a) To provide democratic and accountable government for local communities;
b) To ensure the provision of services to communities in a sustainable manner;
c) To promote social and economic development;
d) To promote a safe and healthy environment;
e) To encourage the involvement of communities and community organisations in the matters of local government.

156. Powers and functions of municipalities

1. A municipality has executive authority in respect of, and has the right to administer.

a) Local government matters listed in part B of schedule 4 and part B of schedule 5; and
b) Any other matter assigned to it by national and provincial legislation

Schedule 4 Part B	Schedule 5 Part B
Air pollution • Building regulations • Child care facilities • Electricity and gas reticulation • Firefighting services • Local tourism • Municipal airports • Municipal planning • Municipal health services • Municipal public transport • Municipal public works • Pontoons, ferries, jetties, piers and harbours, • Storm water management systems in built-up areas • Trading regulations • Water and sanitation services	Beaches and amusement facilities • Billboards and the display of advertisements in public places • Cemeteries, funeral parlours and crematoria • Cleansing • Control of public nuisances • Control of undertakings that sell liquor to the public • Facilities for the accommodation, care and burial of animals • Fencing and fences • Licensing of dogs • Licensing and control of undertakings that sell food to the public • Local amenities • Local sport facilities • Markets • Municipal abattoirs • Municipal parks and recreation • Municipal roads • Noise pollution • Pounds • Public places • Refuse removal, refuse dumps and solid waste disposal • Street trading • Street lighting • Traffic and parking

Unfunded Mandates

An unfunded (or underfunded) mandate is when a sphere of government performs certain functions or activities for which it has no (or inadequate) funds. Municipalities carry out functions that are not included in the powers and functions allocated to them by the Constitution or Legislation, while policy decisions made at national level result in provinces and municipalities facing underfunded or unfunded mandates.

The reasons for such situations include:

Historical roles assumed in the past (for example by certain municipalities), which have continued into new constitutional era.

Weak, incomplete or confused allocation of functions, the result of poor policy making and oversight.

Implicit or explicit choice by a sphere of government to perform a function.

Unfunded or underfunded mandates have implication for the equitable sharing of national revenue and delivery of services. (Financial and Fiscal Commission 2011)

Physical Environment

Madibeng municipality functions within a physical environment which covers a total surface area of 3839 km². Madibeng is demarcated into 36 wards which consists of several urban areas, rural areas, villages, farm portions, as well as a properly established and serviced industrial area. With the ever growing population, the physical environment is bound to change which is to be considered for risk management purposes.

Internal and external Organisational Environment

Madibeng Municipality does not operate in a vacuum, it affects and is affected by decisions made by itself and a multitude of external organisations such as:

a) The Council
b) Provincial Government
c) District Municipality
d) National Treasury
e) Eskom
f) Media
g) Auditor General, Internal Audit and Audit Committees
h) Business Community, etc.

Uncertainty of the Future

It is becoming increasingly difficult for the management of a municipality to accurately predict the future, to anticipate future threats and weaknesses and the negative impact these can have on the municipality and all of its stakeholders.

It has become necessary to adopt a firm position on how the uncertainty of the future and the adverse implication that it may hold can be managed in the most effective, efficient and proactive way possible and to protect the municipality and its stakeholders against any possible future adverse and unforeseen occurrence.

Prevention, minimisation, and avoidance are often simpler, less painful, less costly and more successful than cure.

RISK MANAGEMENT STRATEGY & POLICY

Introduction and background

1.1 The risk management concept in the Public Sector is founded on the principles of *"Batho Pele"*. The *"Batho Pele"* principles link directly with section 195 of the Constitution of the Republic of South Africa, Act 108 of 1996, both of which are aimed at improving performance on service delivery.

1.2 Fundamental to "Batho Pele" principles and the aforesaid section of the Constitution of the Republic of South Africa is that they are based on the values of efficient, effective and economical utilisation of resources, all of which relates to the importance of competent human resource to ensure that Madibeng Local Municipality is having a prudent approach to risk management.

1.3 Risk is inherent in all functions undertaken by or on behalf of Madibeng Local Municipality. All personnel are responsible for managing the risks that relate to their particular area of work. Risks should be managed in a way that derives the best outcome for the municipality and its stakeholders.

1.4 Madibeng Local Municipality functions in an open high risk environment where not only its own actions but those of all role players and stakeholders can negatively impact on the manner in which it operates. How this function is managed can significantly affect the community, district, provincial and national interests as well as municipal reputation.

1.5 Risk management must be an integral proactive component of the corporate management process comprising of risk identification, prevention, minimisation, avoidance and cure.

1.6 Risk management is a systematic process to identify risks to the municipality in achieving its strategic objectives as determined in the integral development plan. It is an integral part of the approach to decision

making and accountability, comprising the organisational culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects within the municipal environment.

1.7 The intention of this policy cannot be to eliminate all risks to the municipality. It is to assist personnel to manage the risks involved in all activities to maximise opportunities and minimise adverse consequences. Effective risk management requires:

a) A systematic process that should be used when making decisions to improve the effectiveness and efficiency of managing risks
b) Taking action to minimise risks
c) Identifying and exploiting opportunities identified during the risk management processes
d) Risk management planning
e) Effective communication
f) Balance between the cost of managing risk and the anticipated benefits.
g) Systems (structures, Risk Register, Risk Management Standard Operating Procedure, Information Technology), etc.

Uncertainty
o Municipalities operate in environments where factors such as technology, regulation, restructuring, changing service requirements and political influence create uncertainty.
o Uncertainty emanates from an inability to precisely determine the likelihood that potential events will occur and the associated outcomes.

Objectives of Risk Management

Risk management aims to address multiple objectives:

1.1 Inform and facilitate
    1.1.1 Effective risk management affects everyone in the municipality. To ensure a widespread understanding, executive management and all departmental managers, staff and councillors should be familiar with the principles set out in this policy.

1.2 Strategic Alignment
    1.2.1 Risk management activities will be aligned to the integrated development plan projects, plans, objectives and priorities. It will

encompass all strategic and operational risks that may prevent the municipality from achieving its objectives.

1.3 Mitigate
1.3.1 The municipality will anticipate and take preventative action to avoid risks rather than dealing with consequences.
1.3.2 A consistent approach to the identification, assessment and management of risks will be embedded throughout the municipality.
1.3.3 Risk control and mitigating measures will be effective, appropriate, proportionate, affordable and flexible.
1.3.4 Risk controls will not be implemented where the cost and effort is disproportionate to the expected benefits.
1.3.5 The municipality will commit the necessary resources to implement risk management consistent with the above principles.

1.4 Set Risk Management Standards
1.4.1 The policy sets the standard at which the Municipality intends and expects risk to be managed and accordingly ensures that such a required standard is known and set for the organisation.

1.5 Monitor and Review
1.5.1 The policy sets standards, processes and responsibilities to make it possible to monitor the extent that risk management responsibility is met. This includes the assessment of whether the risk management strategy is producing the sustainable outcomes as originally envisaged.

1.6 Compliance
1.6.1 This policy aims to achieve compliance and to implement best practices in support of section 62 (1) (c) (i) of the Municipal Finance Management Act.
1.6.2 To avoid future audit findings, risk management must be performed to its maximum level which includes adoption and implementation of the Risk Management Policy.

1.7 Risk Awareness
1.7.1 The municipality will conduct workshops at least twice per year and parallel to the budget and SDBIP review, in order to spread the necessary level of understanding by the Executive Mayor, the

Councillors, the Municipal Manager, the directors and all other relevant officials.

1.7.2 The executive management will embrace a culture of risk awareness at the top level.

1.8 Safeguarding of Municipal Resources

1.8.1 Safeguard MLM's resources by assessing risk of ineffective controls to encourage efficient, reliable and cost-effective delivery of services and optimal utilisation of resources.

1.9 Advice in decision making processes

1.9.1 Support the effective functioning of core business processes and allow more reliable decision making through assessing risk in key management agenda items.

Policy Statement

It is the policy of Madibeng Local Municipality to adopt a common approach to the management of risk. This approach involves a clearly stipulated strategy defining the risks that the municipality is exposed to and the manner in which the risks shall be managed. The municipality will identify and manage its risk in support of its vision, mission, goals and aims as set out in the Integrated Development Plan (IDP), Service Delivery and Budget Implementation Plan (SDBIP) and its operations.

The risk policy guide the development of a strategic plan that should address the following:
An effective risk management architecture,
A reporting system to facilitate risk reporting and
An effective culture of risk management.

The municipality will promote the risk management language and culture in all sections of the municipality and aim to demonstrate quality improvement resulting from effective risk management.

Madibeng Local Municipality is committed and determined to adequately manage risks in a proper, proactive, on-going and positive manner.

The aforesaid scenario will be made possible by providing a framework for the effective identification, evaluation, management and reporting lines of Municipality's risks, and by inculcating the culture of corporate governance, excellence, creativity, team work and adaption to changes in the discipline of risk management.

Purpose and Scope of Application

1.1 The purpose of this policy is to outline the Municipality's position and approach to risk management. This is done by clearly defining the basis for risk management framework and the manner in which to identify and address potential risks, and the role to be played by different role players.

1.2 To ensure that there is an understanding of risk management framework. Therefore this policy applies to the institution as a whole.

Risk Function and Activities

1.1 Risk defined

The uncertainty of an event occurring that could have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.

1.2 Risk Management

It is a systematic process which is applied to identify, evaluate and address risks on a continuous basis before such risks can impact negatively on the service delivery capacity of the Municipality, and that monitoring is key to the process itself because it is aimed at checking the progress in carrying out mitigating strategies to reduce the magnitude of risks. It forms part of management's core responsibilities and is an integral part of internal processes of the Municipality.

Risk Management is not an ad hoc, once off, reactive or crisis management process and will be performed in a structured and formal manner at least twice a year to reflect the current state of risk management within the municipality. The risk planning review process will include;

a) The review of the risk management policy
b) Appraisal of the risk management committees
    i. Effectiveness
    ii. Performance
    iii. Structure
    iv. Reporting
c) Review of risk management structures
d) Risk workshop to review the risk register
e) Assurance that the internal audit plan is aligned with the risk register
f) Review of the risk management systems

1.3 Control

This is the deliberate action taken to eliminate or minimise risk.

1.4 Impact

This is the effect (consequence) of the risk.

1.5 Inherent risk

This is the intrinsic (natural) risk, which in concise is referred to as the level of risk before any controls are put in place.

1.6 Likelihood

This is the probability used to measure a potential risk that could occur in the Municipality.

1.7 Total residual risk

This is the risk that remains after all possible mitigations (controls) have been implemented. The calculation of total residual risk equals to residual impact multiply by residual likelihood (RI X RL= TRR).

1.8 Risk ranking

This is the process of prioritising risks in terms of their importance.

1.9 Risk register

It is a template containing in it all relevant information of the identified

risks such as: key performance areas of the Municipality, risk number, Description of risk and etcetera.

1.10 Risk evaluation template or register for updating risks

It is a template utilised to monitor progress made on identified risks. It is important that this tool should be accompanied by a portfolio of evidence as a basis of providing reasonable assurance that indeed progress is made with regard to identified risks.

1.11 Risk response

This is the specific course of action to reduce the likelihood or impact of a risk, such as risk avoidance, risk transfer, risks treatment (retention), risk acceptance and risk exploitation.

Risk profile, risk tolerance and risk appetite

1.1 Risk profile refers to unique characteristics of risks in the Municipality.

1.2 It is imperative on the Municipality to understand the ways and means of profiling risks and these are the areas to be looked at for effective profiling of risks:

1.2.1   a risk should be briefly described;
1.2.2   determine the contributing factors to the risk;
1.2.3   rating of risks in terms of likelihood and impact before consideration of current controls (in its inherent nature);
1.2.4   consideration of current controls;
1.2.5   guidelines on the rating of perceived control effectiveness;
1.2.6   rating of risks after consideration of current controls (residual risk rating); and
1.2.7   to provide a list of mitigating plans of risks with timelines and risk owners and the frequency of reporting to the Risk Management Committee.

1.3 Risk tolerance refers to the level of risk exposure that is acceptable. When a certain level of risk is tolerable a conscious decision is made not to control that portion of risk. This will mean that anything above the tolerance level will have to receive urgent action by management, hence it may result to

negative outcomes and as a result hinders the Municipality in achieving its set objectives.

1.4 It is the council's responsibility to determine the risk appetite in its various areas of operation. The risk appetite should be clearly stated and articulated so that it informs management decisions. As a principle, and in support of the Municipal Finance Management Act, the municipality shall have a low risk appetite for all forms of loss resulting from negligence and fruitless or wasteful expenditure. Senior management with the assistance of Performance Management Systems, Internal Audit and Risk Management departments will endeavour to determine the risk appetite of each department under their control.

Risk appetite can be defined as the amount of risk that the municipality is willing to accept in pursuit of its vision and mission. The risk appetite guide the allocation of resources. Management allocates resources across functional areas with consideration of the municipal risk appetite and unit plans for ensuring that objectives are met whilst containing expenditure within the budget. Management considers its risk appetite as it aligns the municipality, its people and processes and designs the infrastructure to effectively respond to and monitor risks.

Risk appetite enables an improved consistency of decision making at all levels through improving risk understanding and also provides a framework for knowingly taking risks within boundaries. The risk appetite 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 setting the strategy, with capital expenditure and other strategic decisions reviewed against it as they arise.

The key determinants of risk appetite are as follows:
1. Expected performance
2. The capital needed to support risk taking
3. The culture of the municipality
4. Management experience along with risk and control management skills
5. 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, it should be reviewed by management and the accounting officer on an annual basis.

Risk Assessment

The risk assessment is a systematic process to quantify or qualify the level of risk associated with a specific threat or event. The main purpose of risk assessment is to help management to prioritise the identified risks. This enables management to spend more time, effort and resources to manage risks of higher priority than risks of lower priority. The output of the risk assessment is a risk register enriched by the addition ratings for each risk.

Risk should be assessed on the basis of the likelihood of the risk occurring and the impact of its occurrence on the particular objective it is likely to affect. The risk assessment is performed using a 3 step process.

Step 1: Develop the scoring system for Impact and Likelihood before the actual assessment.

The following is a rating table that is utilised to assess the impact of risk:

Rating	Impact	Definition
5	Critical	Negative outcomes or missed opportunities that are of critical importance to the achievement of the objective. It is very unlikely that this objective will be achieved 1-29%
4	Major	Negative outcomes or missed opportunities that are likely to have a relatively substantial impact on the ability to meet objectives. It is very unlikely that this objective will be achieved 30-49%
3	Moderate	Negative outcomes or missed opportunities that are likely a relatively moderate impact on the ability to meet objectives. The objective may be achieved 50-69%
2	Minor	Negative outcomes or missed opportunities that are likely to have a relatively low impact on the ability to meet the objectives. It is likely that this objective will be achieved 70-89%
1	Insignificant	Negative outcomes or missed opportunities that are likely to have a negligible impact on the ability to meet objectives. The objective will certainly be achieved 90-100%

The following is a rating table that is utilised to assess the likelihood of risks:

Rating	Impact	Definition
5	Almost certain	The risk is already occurring, or is likely to occur more than once within the next 12 months. There's a 90-100% chance that this risk will definitely occur.
4	Likely	The risk could easily occur, and is likely to occur at least once within the next 12 months. There's a 70-89% chance that this risk will occur.
3	Moderate	There is an above average chance that the risk will occur at least once in the next three years. There is a 50-69% chance that this risk may occur.
2	Unlikely	The risk occurs infrequently and is unlikely to occur within the next 3 years. There's a 30-49% chance that this risk will not occur.
1	Rare	The risk is conceivable but is only likely to occur in extreme circumstances. There's a 1-29% chance that the risk will not occur.

Illustrated quantitative and qualitative measurement criteria:

Impact is the potential loss to the organisation or the service delivery failure should be risk materialise. The following impact criteria will be used:

Details	Insignificant	Minor	Moderate	Major	Critical
Value "R"	0 – 5,000	5,001–20 000	20,001–100,000	100,001-500,000	500,000+
Reputation	Internal	Local Press	Provincial Press	National Press	International Press
Time	1-2 days	1-4 weeks	1-3 months	3-6 months	6 months+

Likelihood is the probability that an event, which could have an impact on the organisation achieving its objectives, may occur. The following likelihood criterion will be used:

Details	Minimum	Low	Medium	High	Maximum
Percentage	≤ 10%	10-25%	26-50%	50-90%	≥90%

Step 2: Apply the scores to the risk matrix to indicate what areas of the matrix would be regarded as high, medium or low risk.

$$\text{Risk index} = \text{impact} \times \text{likelihood}$$

IMPACT	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5

LIKELIHOOD

↓

Risk Index	Risk Magnitude
13-25	High
6-12	Medium
1-5	Low

Step 3: Determine the acceptability of the risk and what action will be proposed to reduce the risk.

Risk index	Risk Magnitude	Risk Acceptability	Proposed Actions
13-25	High Risk	Unacceptable	High Level of control intervention required to achieve an acceptable level of residual risk.
6-12	Medium Risk	Unacceptable	Unacceptable except under unique circumstances or conditions. Moderate level of control intervention required to achieve an acceptable level of residual risk.
1-5	Low Risk	Acceptable	Low level of control intervention required, if any.

Risk assessment is applied first to inherent risk – the risk to the municipality in the absence of any action management might take to alter either the risk's likelihood or impact. Then the residual risk is established to determine the actual level of risk after the mitigating effects of management actions to influence the risk.

The following diagram differentiates between inherent and residual risk.

Inherent and Residual Risk

Inherent Risk – Before the assessment of controls

Residual Risk – After the assessment of controls
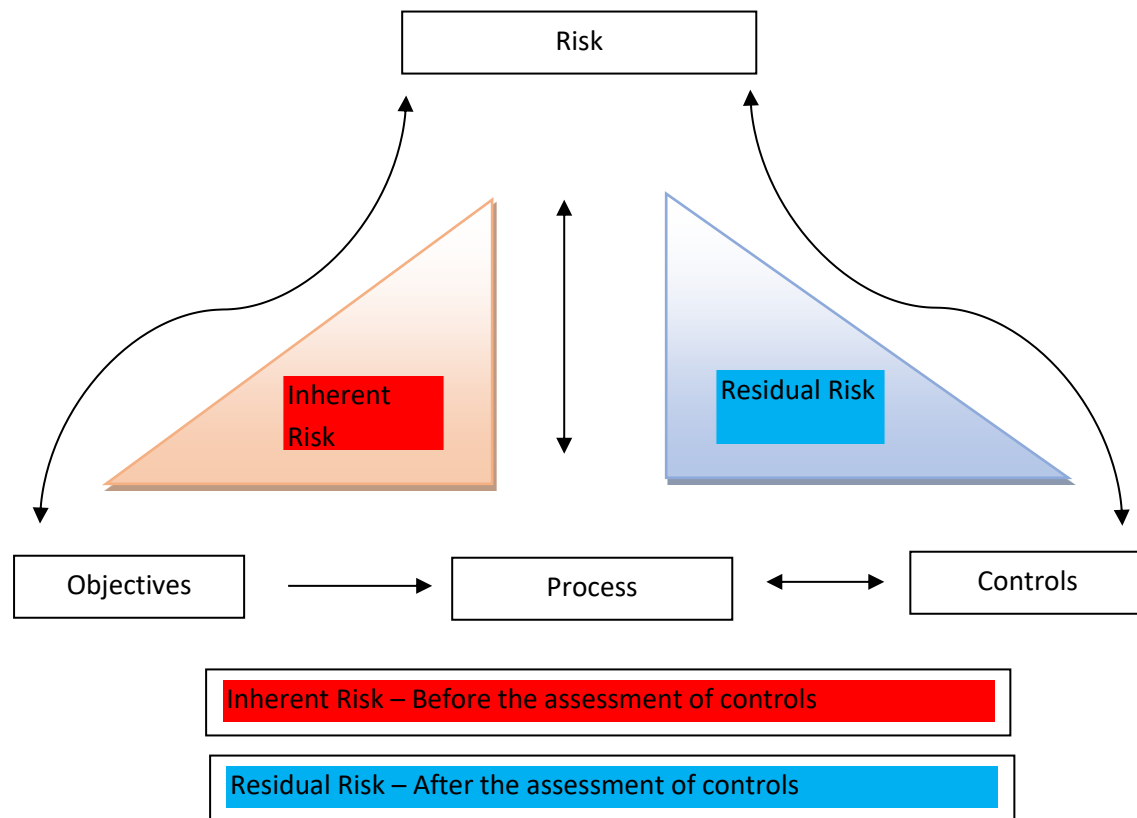
Risk Response

Risk response is concerned with developing strategies to reduce or eliminate the threats and events that create risks. Risk response involves identifying and evaluating the range of possible options to address and implementing the chosen option.

Management should develop response strategies for all material risks, prioritising the risks exceeding or nearing the risk appetite level. Response strategies should be documented together with the responsibilities and timelines.

Risk responses fall within the following categories:

Category	Description

Avoid	Refrain from engaging in activities that may result in loss exposure.
Treat	Manage the risk. Management undertakes to implement actions that are designed to reduce the likelihood, impact or both.
Transfer	Steps taken to shift the loss of liability to third parties such as insuring and outsourcing
Terminate	Management takes action to remove activities that gave rise to the risks
Tolerate	Management accepts the risk. Informed decision to accept both the impact and likelihood of risk events

The residual risk exposure (inherent risk X control effectiveness)

Risk Rating	Residual Risk Magnitude	Response
13-25	High	Unacceptable level of residual risk. Implies that the controls are either fundamentally inadequate (poor design) or ineffective (poor implementation). Controls require substantial redesign or a greater emphasis on proper implementation.
6-12	Medium	Unacceptable level of residual risk. Implies that the controls are either inadequate (poor design) or ineffective (poor implementation). Controls require some redesign or a more emphasis on proper implementation.
1-5	Low	Mostly acceptable level of residual risk. Requires minimal control improvements

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 a municipality strives to achieve its objectives.

Control activities are the policies and procedures that help ensure that management responses are properly executed. They occur throughout the municipality, at all levels and in all functions.

Management is responsible for designing, implementing and monitoring the effective functioning of the system of internal controls. Without derogating from the above, everyone in the municipality should also have responsibilities for maintaining effective system of internal controls, consistent with their delegated authority.

Management should develop the internal control architecture through:
- Preventative controls to prevent errors or irregularities from occurring e.g. physical security of assets to prevent theft;
- Detective controls to find errors or irregularities after they have occurred e.g. performance of reconciliation procedure to identify errors; and
- Corrective controls that operate together with detective controls to control errors and irregularities.

The internal controls architecture should include:
- Management controls to ensure that the municipality's structure and systems support its policies, plans and objectives, and that it operates within laws and regulations;
- Administrative controls to ensure that policies and objectives are implemented in an efficient and effective manner;
- Accounting controls to ensure that resources are accounted for fully and transparently and are properly documented; and
- Information technology controls to ensure security, integrity and availability of information

Perceived control effectiveness

Effectiveness category	Category definition	factor

Very good	Risk exposure is effectively controlled and managed	20%
Good	Majority of risk exposure is effectively controlled and managed	40%
Satisfactory	There is room for some improvements	65%
Weak	Some of the risk exposure appears to be controlled, but there are major deficiencies	80%
Unsatisfactory	Control measures are inherent	90%

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 will be applied at all levels across the municipality.

Monitoring activities should focus on:
- Monitoring of risk action plans – risk plans need to be monitored on an ongoing basis to ensure the necessary actions are implemented on schedule and as intended.
- Monitoring of new and emerging risks – the risk profile of any organisation will change over time. Thus there is a need to monitor and review the risk profile of the municipality to ensure that it remains relevant and complete. Changes in strategy, the legal and regulatory environment, restructuring, loss of key personnel, significant control deficiencies, fraud, changes in business objectives will require an immediate review of the municipal risk profile.
- Monitoring of the effectiveness of the risk management process – the efficiency of the entire risk management process should be monitored periodically. A positive correlation should exist between improvements in the system of risk management as well as institutional performance.

Incident reporting
Incident reporting is another means of risk monitoring and reviewing the effectiveness of controls. Certain disciplines such as Safety, Health Environment and Quality may already have in place incident reporting systems. Such reporting systems should be

integrated into the broader risk management incident reporting system in order to avoid duplication of effort.

Performance measurement

Management's performance with the processes of risk management will be measured and monitored through the following performance management activities:

1. Monitoring of progress made by management with the implementation of risk management frame work;
2. Monitoring of loss and incident data;
3. Management's progress made with risk mitigating action plans; and
4. An annual quality assurance review of risk management performance.

Accountability for Risk Management

The detailed line accountability for risk management is fully aligned with the Municipality's management structure. Accordingly, the approvals, responsibilities and accountabilities applicable to the identification, evaluation/analysis, treatment and results and reporting of the Municipal risks are attributed to the Accounting Officer and the Risk Management Unit.

The Accounting Officer and the Chief Risk Officer are responsible for the ultimate signing of all risk information to the Council and Audit Committee for review.

Reporting

New risks and changes to existing risks will be captured into risk management system in the month they are identified. The information relating to new risks and/or changes to the existing risks should be communicated by the Risk Owner to the Risk Management Department.

The Risk Management Department will collect and aggregate the information and will report to the Accounting Officer, monthly, regarding the risk profile of the Municipality.

The Accounting Officer, assisted by the respective Heads of Departments will report to the Council as and when required, both the current risk profile and a summary of any major changes since the last report.

Review

The Risk Management Department led by the Chief Risk Officer will coordinate an annual review of the effectiveness of this framework as well as all organisational risks, uninsured and uninsurable risks together with the key managers in the Municipality. This annual review will take place immediately prior to the development of the annual business and integrated development plans so that it can have due regard to the current as well as the emerging risk profile of the business.

Internal Audit will monitor key controls identified in the risk management system as part of the annual audit plan developed in conjunction with the Accounting Officer and approved by the Audit Committee.

The Municipality will review the risk profile in developing their recommendations to the Council regarding the Municipality's risk financing policy and strategy.

Roles and Responsibilities

Every employee is responsible for executing the risk management process and adhering to the risk management procedures laid down by Management in their areas of responsibility.
The parties that have a significant role to play in the process of risk management are set out below:

Legends

| OVERSIGHT ROLE | ASSURANCE ROLE | IMPLEMENTOR | SUPPORT |

10.1. Audit Committee

No.	Responsibilities	Accountability	Frequency
1	To meet at least 4 times a year with risk as a standard agenda item	Chairperson	Quarterly
2	Monitor the municipality's risk management process	Chairperson	Annually
3	Assessment on the effectiveness of risk management for inclusion in the annual report MFMA, section 166 (2)(a)(ii)	Chairperson	Continuous
4	Ensuring that the internal audit plans are aligned to MLM's risk profile	Chairperson	Annually
5	Satisfy itself that it has appropriately addressed the following areas - financial reporting risks, including the risks that relates to fraud;	Chairperson	Continuous

	- internal financial controls; and - IT risks as they relate to financial reporting.		
6	Review and recommend disclosures on matters of risk in the annual financial statements;	Chairperson	Annually
7	Providing a regular feedback to the Accounting Officer on the adequacy and effectiveness of risk management in the municipality, including recommendations for improvement;	Chairperson	Quarterly

10.2. Accounting Officer

No.	Responsibilities	Accountability	Frequency
1	Setting a tone at the top by supporting and being seen to be supporting the institution's aspirations for effective management of risks;	MM	Continuous
2	Delegating responsibilities for risk management to management and internal oversight structure such as the Risk Management Committee;	MM & Executive Management	Quarterly
3	Holding management accountable for designing, implementing, monitoring and integrating risk management into their day-to-day activities;	MM & Executive Management	Continuous
4	Providing leadership and guidance to enable management and internal structures responsible for various aspects of risk management to properly perform their functions;	MM	Continuous

5	Ensuring that the control environment is conducive for effective functioning of risk management;	MM	Continuous
6	Approving the municipality's risk tolerance and appetite;	MM	Continuous
7	Devote personal attention to overseeing management of significant risks;	MM	Continuous
8	Ensuring appropriate action in respect of recommendations by the Audit Committee, internal and external audits and Risk Management Committee to improve risk management;	MM & Executive Management	Continuous
9	Providing assurance to relevant stakeholders that key risks are properly identified, assessed and mitigated.	MM & Executive Management	Continuous
10	Ensure that risk management is a standing item in all management meetings and that Heads of Departments report on their risks within their departments	MM & Executive Management	Continuous

10.3. Chief Financial Officer

No.	Responsibilities	Accountability	Frequency

1	Annual review of the disaster recovery and business continuity plans	CFO & Executive Management	Annual
2	Same duties and/or responsibilities which are assigned to management as mentioned below.	CFO	Continuous

10.4. Executive Management / Directors

No.	Responsibilities	Accountability	Frequency
1	Managers are responsible for ensuring the achievement of objectives in the areas of their responsibility and should for these purposes identify issues that could prevent them from achieving their goals, thus in short, managers are responsible for managing the risks within their areas of responsibility. They should ensure that other officials carry out their duties;	Executive Management / Directors	Continuous
2	Management is responsible for implementing risk management systems within their areas of responsibility by identifying risks that are within their line functions;	Executive Management / Directors	Continuous
3	Empowering officials to effectively perform risk management responsibilities through proper communication of their responsibilities,	Executive Management / Directors	Continuous
4	Aligning the functional risk management methodologies and processes with MLM's processes;	Executive Management / Directors	Bi-annual
5	Devoting personal attention to overseeing the management of key risks within their areas of responsibility;	Executive Management / Directors	Continuous

6	Monitoring risk management within their area of responsibility, and holding officials responsible for their specific risk management responsibilities.	Executive Management / Directors	Continuous
7	Maintaining a proper functioning of the control environment within their areas of responsibility;	Executive Management / Directors	Continuous
8	Providing risk management reports on the status of the identified risks;	Executive Management / Directors	Continuous
9	Presenting to the Risk Management and Audit Committees when requested to do so;	Executive Management / Directors	Continuous
10	Maintain a co-operative relationship with the Risk Management Division and Risk Champions;	Executive Management / Directors	Continuous

10.5. Chief Risk Officer

No.	Responsibilities	Accountability	Frequency
1	9.6.1 The role of the Chief Risk Officer is to manage the Risk Management Division and ensure that risk inputs from departments are assimilated and passed through to the Municipal Manager through the Risk Management Committee and the Audit Committee. The role of this function is to set policies and standards for risk management, risk reporting and the integrity of the risk management processes.	CRO	Continuous
2	In addition, the key responsibilities of the CRO include:	CRO	Continuous

	(a) working with senior management to develop the municipality's vision for risk management;
	(b) developing, in consultation with management the municipality's risk management framework incorporating *, inter alia*, the:
	  i) risk management policy;
	  ii) risk management strategy;
	  iii) risk management implementation plan;
	  iv) risk identification and assessment methodology;
	  v) risk appetite and tolerance; and
	  vi) Risk classification.		

3	Communicating the municipality's risk framework to all stakeholders in the institution and monitoring its implementation;	CRO	Continuous
4	Facilitate orientation and training for the Risk Management Committee;	CRO	Bi-annual
5	Training all stakeholders in their risk management functions;	CRO	Continuous
6	Continuously driving risk management to higher levels of maturity;	CRO	Continuous
7	Assisting management with risk identification, assessment and developing of response strategies;	CRO	Continuous
8	Monitoring the implementation of the response strategies; collating, aggregating, interpreting and analysing the results of the risk assessments to produce a risk register;	CRO	Continuous

9	Reporting the risk register to the Accounting Officer, Management and Risk Management Committee; and participating with Internal Audit, Management and Auditor-General South Africa in developing the combined assurance plan for the municipality; and	CRO	Continuous
10	Shall convene a meeting with risk champions on monthly basis to obtain monthly departmental risks mitigating reports in order to check progress made and that the CRO shall ensure capacity building of the risk champions.	CRO	Continuous

10.6 Internal Audit

No.	Responsibilities	Accountability	Frequency
1	The Internal Audit will adhere to section 165 (2) (a) of the MFMA by designing a risk based audit plan and an internal audit program for each financial year through the use of the municipality's risk register and other sources. The Risk Management Division shall develop a risk register to be used as basis for developing Internal Audit Plans. The Municipality's risk register will be used to identify extremely risky areas and thereafter review the identified areas to verify whether there are internal controls in place and whether they are effective and working as intended; and *After reviewing the different functional areas, the Internal Audit*	CAE	Continuous

| | *will* collaborate with Risk Management Division to resolve the identified internal control deficiencies. The Risk Management Division will thereafter assist management in designing controls that are aimed at ensuring that the identified weaknesses are properly addressed.

Once the abovementioned process has been completed and implemented, the Internal Audit will perform a follow-up audit to verify whether the designed internal controls are working as intended. The Risk Management Division will evaluate reports from Internal Audit to assess the effectiveness of the designed controls. | | |
|---|---|---|---|
| 2 | Utilise risk assessment report to compile its strategic and operational audit plans; | CAE | Annually |
| 3 | Provide inputs to the risk manager for the annual risk assessment; | CAE | Bi Annual |
| 4 | Formally review the effectiveness of risk management processes. | CAE | Annually |

10.7. Risk Management Committee

No.	Responsibilities	Accountability	Frequency
1	The Risk Management Committee (RMC) should be appointed by the Accounting Officer to assist the Municipality in discharging its responsibilities over risk management. The membership of the	Chairperson & RMC members	Once off

	committee should comprise both management and external members with the necessary blend of skills, competencies and attributes.		

2	The Chairperson of the Risk Management Committee should be an independent external person appointed by the Accounting Officer; and the following are the areas to be under the control of the above Committee:
	a) Review and recommend for the approval of the following enablers:
	  i) risk management policy;
	  ii) risk management strategy;
	  iii) risk management implementation plan;
	  iv) municipality's risk appetite, ensuring that limits are:
	    • supported by rigorous analysis;
	    • set for all significant risks individually as well as in aggregate for particular categorisation of risks; and
	    • Consistent with the materiality and significance framework.
	  v) municipality's risk tolerance level that it is supported by rigorous analysis of:
	    • the municipality's ability to withstand significant risks; and
	    • The municipality's ability to recover financially and operationally from significant risks.
	  vi) The municipality's risk identification and assessment
		Chairperson & RMC members	Annually

	methodologies, after satisfying itself of their effectiveness in timeous and accurate mechanism of identifying and assessing the municipality's risks.		
3	Evaluate the extent and effectiveness of risk management's integration within the municipality;	Chairperson & RMC members	Monthly/ Adhoc
4	Assess implementation of risk management policy and strategy (including the plan);	Chairperson & RMC members	Monthly/ Adhoc
5	Evaluate the effectiveness of the mitigation strategies implemented to address the Municipality's significant risks;	Chairperson & RMC members	Monthly/ Adhoc
6	Review the material findings and recommendations by the assurance providers on the system of risk management and monitor the implementation of such recommendations,	Chairperson & RMC members	Monthly/ Adhoc
7	Develop its own performance indicators for approval by the Accounting Officer;	Chairperson & RMC members	Monthly/ Adhoc
8	Interact with the Audit Committee to share information relating to the municipality's significant risks; and	Chairperson & RMC members	Monthly/ Adhoc
9	Provide timely and useful reports to the Accounting Officer on the state of risk management together with recommendations to address any deficiencies identified by the committee.	Chairperson & RMC members	Monthly/ Adhoc

10.8. Director Corporate Support Services – ICT

No.	Responsibilities	Accountability	Frequency
1	Develop and implement the disaster recovery and business continuity plans	Director CSS & ICT Manager	Continuous

2	Development of an integrated operating systems	Director CSS & ICT Manager	Continuous
3	Same duties and/or responsibilities which are assigned to management as mentioned below.	Director CSS	Continuous
4	Annual review of the disaster recovery and business continuity plans	Director CSS & ICT Manager	Annual

10.9. Council

No.	Responsibilities	Accountability	Frequency
1	Ensuring that the institution's strategies are aligned to the government's mandate;	Council	Quarterly / Adhoc
2	Obtain assurance from management that the municipality's strategies were based on a rigorous assessment of risk;	Council	Quarterly / Adhoc
3	Obtain assurance that key risks inherent in the institution's strategies were identified and assessed, and that they are properly managed;	Council	Quarterly / Adhoc
4	Assist the Accounting Officer to deal with fiscal, intergovernmental, political and other risks beyond his direct control and influence;	Council	Quarterly / Adhoc
5	Insisting on the achievement of the objectives; and	Council	Quarterly / Adhoc
6	Approve the risk management policy, strategy, risk management committee charter, strategic risk assessment	Council	Quarterly / Adhoc

	reports; and other risk management enabling documents.		

10.10 Risk Champions

No.	Responsibilities	Accountability	Frequency
1	A Risk Champion is a person with skills, knowledge, and leadership qualities and power of the office required to champion a particular aspect of risk management;	Executive Managers & Risk Champions	Continuous
2	Intervene in instances where the Risk Management Division's efforts are being hampered, for example , by the lack of co-operation by management and other officials;	Executive Managers & Risk Champions	Continuous
3	Add value to the risk management process by providing support to manage "problematic" risks and risks of transversal nature that requires a multiple participant approach;	Executive Managers & Risk Champions	Continuous
4	Shall provide the CRO with the monthly mitigating reports.	Executive Managers & Risk Champions	Monthly

Other Assurance Providers

Assurance provider such as the Auditor-General South Africa will review different aspects of MLM's operations and activities. These reviews by nature will address risk management's effectiveness. It should be noted that the scope and mandates of the activities of assurance providers are established separately from the risk management policy.

Safety, Health and Environment

A formal safety management programme is essential for the municipality. The scope of the safety management programme should include administrative

aspects, safety awareness and training, health, hygiene, electrical safety, physical safety, micro environmental exposures and legislative requirements.

Compliance

Compliance is a key element of the risk management process. All statutory compliance obligations must be managed to an acceptable level.

Business Continuity Management

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

Fraud Plan

Madibeng Local Municipality is responsible for the establishment of its own fraud prevention policy and plan. Confidential reporting of potential breaches and actual investigations should be reported to the Risk Management Committee.

Risk Implementation Plan

The Enterprise Risk Management Unit shall on an annual basis develop for approval of the Risk Management Committee a Risk Management Implementation Plan which should highlight the following areas:

1. Key Performance Area
2. Performance Target
3. Performance Indicator
4. Due Date, and
5. Responsible Person

Risk Management Performance Awards

Risk Management awards are a form of honour, a kind of recognition aimed to felicitate department's and/or one's outstanding contribution in risk management processes. Risk Management awards are not only a great prestige or a mark of excellence, but are also a tremendous boost for departments and risk champs to strive and excel higher and aim for even bigger accomplishments in legislative mandate of service delivery.

Categories to be are:

1. A leading department in risk management,
2. The most dedicated Risk Champion and
3. The most improved Risk champion

The criterion used to identify the above awardees is as follows:

1. **A leading department in risk management** is as follows

Bases	Weight
Implementation of risk treatment plans/mitigation strategies	50%
Compliance reporting	25%
Attendance of RMC by the director	25%

2. **The most dedicated Department (Risk Champion)** is as follows

Bases	Weight
Consistency of implementation of risk treatment plans/mitigation strategies by the department	15%
Consistency of compliance in reporting by the department	45%
Risk Champion's consistency of attending RMC and ERM convened meetings	40%

3. **The most improved Department (Risk Champion)** is as follows

Bases	Weight
If a department have received award(s) for 1 and/or 2 is automatically disqualified for this category	

Implementation of risk treatment plans/mitigation strategies by the department from midterm to financial year end	15%
Compliance reporting by the department from midterm to financial year end	45%
Risk Champion's attendance of RMC and ERM convened meetings	40%

Review of the policy

The policy will be reviewed annually or whenever a need arises.

Conclusion

The strict implementation and the compliance to this risk management policy will assist Madibeng Local Municipality to adequately reduce consequences of risks. This policy seeks to outline how the Council should go about in dealing with specific types of risks and also improve our partnership working arrangements and corporate governance principles.

RISK MANAGEMENT STANDARD OPERATING PROCEDURES

Risk Identification and Assessment

1. Introduction

Risk assessment is a systematic process to qualify the level of risk associated with a specific threat or event, to enrich the value of risk information available to the municipality. The main purpose of risk assessment is to help the municipality to prioritise the most important risks, as the Municipality is not expected to have the capacity to deal with all risks in an equal manner.

Risk assessment provides an understanding of risks, their causes, consequences and their probabilities. This provides input to decisions about:

a) Whether an activity should be undertaken;
b) How to maximise opportunities;
c) Whether risks need to be treated
d) Choosing between options with different risks;
e) Prioritising risk treatment options; and
f) The most appropriate selection of risk treatment strategies that will bring adverse risks to a tolerable level

2. The purpose of a risk assessment

The purpose of risk assessment is to provide evidence-based information and analysis to make informed decision on how to treat particular risk and how to select between options. Some of the principal benefits of performing risk assessment include:

a) Understanding the risk and its potential impact upon objectives;
b) Providing information for decision makers;
c) Understanding of risks, in order to assist in selection of treatment options;
d) Identification the contribution to risk and weak links in systems and municipality;
e) Comparing of risks in alternative systems, technologies or approaches;
f) Communicating risks and uncertainties
g) Assisting with establishing priorities;
h) Contributing towards incident prevention through post-incident investigation;
i) Selecting different forms of risk treatment;
j) Meeting regulatory requirements;
k) Providing information that will help evaluate whether the risk should be accepted when compared with pre-defined criteria.

3. The risk assessment process

Risks should be assessed on the basis of the likelihood of the risks occurring and the impact of its occurrence on the particular objective(s) it is likely to affect. Risk should be expressed in the same unit of measure used for key performance indicator(s) concerned. In simplified terms, there should be high correlation between key performance indicators and key risk indicators.

Risk assessment should be performed through a three stage process:

a) Firstly, the inherent risk should be assessed to establish the level of exposure in the absence of deliberate management action to influence the risk;

b) Secondly, a residual risk assessment should be performed to determine the actual remaining level of risk after the mitigating effects of management actions to influence the risk; and

c) Thirdly, the residual risk should be benchmarked against the Municipality's risk appetite to determine the need for further management intervention, if any.

Risk assessment should be strengthened by supplementing management's perception risk, inter alia with:

a) Review of the reports to the Audit Committee:

b) Financial analyses, including of liquidity and Solvency analysis;

c) Historic data analyses, Which might include audit report and incident reports and actual loss data;

d) Interrogation of trends in key performance indicator;

e) Benchmarking against municipality of the same nature and size;

f) Market and economic sector information

g) Scenario analyses; and

h) Forecasting and stress testing.

Risk assessment should be re-performed for the key risk in response to significant environmental and/or municipal changes, but at least once a year, to ascertain the shift in the magnitude of risk and the need for further management action as a result thereof

The outline below summarises the steps of the risk management progress. It normally comprises of five phases namely

Establishing the context	Establishing context is about setting the parameters or boundaries around the risk appetite and risk management activities. It requires consideration of the external factors

	alignment with internal factor such as strategy , resources and capabilities the risk manager will then need to establish context of the risk management progress which includes amongst other things establishing a risk management policy, progresses, methodologies, plans, plans, risk rating criteria, training and reporting progress.
Identify the risk	Comprises of the processes for identifying, analysis and evaluating risks. Ideally, the municipality will utilise a range of risk identification techniques including brainstorming, work breakdown analysis, and expect facilitation.
Analyse the risk	Risk analysis considers possible causes, source, likelihood and consequences to establish the inherent risk. Existing management controls should be identified and effectiveness assessed to determine the level of residual risk.
Assess the risk	After this analysis, an evaluation of the level of risk is required to makes decisions about further risk treatment.
Treat the risk	Where the level of risk remains intolerable, risk treatment is necessary. Risk Owners can treat risks by avoiding the risk, treating the risk source, modifying likelihood, changing consequences or sharing elements of risk. The remaining level of risk retained should be within risk appetite.

4. Risk Context

Risk analysis required a thorough understanding of the risk context, including its internal and external environment and the purpose of risk management activity. It also include assigning roles and responsibilities of various parts of the municipality participating in the risk management process. Understanding the external environment of a municipality involves looking at the impact of the

social, culture, regulatory and political activities when developing risk management criteria.   In this way, it is possible to prepare for external threats and take advantage of externally generated opportunities.

The internal context highlights a municipality's culture, its internal stakeholder, municipality structure, and its human resource capabilities. It looks at a municipality's strategic goals, and its operational fun and processes involving in achieving its objectives   it further include:

a) Policies, objectives, and the strategies that are in place to achieve them;
b) Capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, system, and technologies);
c) Inter-dependencies of the various management system, Function and activities of the municipality;
d) Information systems, information flows and decision-making progress (both formal and informal);
e) Relationships with, and perception and values of, internal stakeholders;
f) The municipality's culture;
g) Standards, guidelines and models adopted by the municipality; and
h) Form and extent of contractual relationships.

This helps a municipality to set a strategic direction for risk management as a key component of the entire municipality's operations. Establishing the context is not a once off step. It is ongoing as it ensure adaptability of municipal risk management to an ever-changing internal and external environment.

5. Risk management context

Establishing the Risk Management Context involves determining the objectives, strategies, scope and parameters of the activities of the municipality. The management of risk should be undertaken with full consideration of the need to justify the resource used in carrying out risk management. The resources required, responsibilities and authorities, and the records to be kept should be specific as part of the risk management context.

The risk management context will vary according to the needs of the municipality and can involve:

a) Defining the goal and objectives of the risk management activities;
b) Defining responsibilities for and within the risk management process;
c) Defining the scope, as well as the depth and breadth of the risk management activities to be carried out, including specific inclusions and exclusions;
d) Defining the activity, process, function , project, product, service, or asset in terms of the time and location;
e) Defining the relationships between a particular project, process or activity and other projects, processes or activities of the municipality;
f) Defining the risk assessment methodologies;
g) Defining the way performance and effectiveness is evaluated in the management of risk;
h) Identifying and specifying the decision that have to be made; and
i) Identifying, scoping or framing studies needed, their extent and objectives, and the resources required for such studies.

6. Risk criteria

A municipality should define criteria to be used to evaluate the significance of risk. The risk criteria should reflect the municipality's values, objective and resources, and key measure of success. I.e. how a municipality will know that it is performing.

Some criteria can be imposed by, or derived from, legal and regulatory requirements and other requirements to which the municipality subscribe. Risk criteria should be consistent with the municipality's risk management policy, be defined at the beginning of any risk management process and be continually reviewed throughout the process.

When defining risk criteria, factors to be considered should include the following:

a) The nature and type of courses and consequences that can occur and how they will be measured (consequence/severity levels the risk rating methodology);
b) How likelihood will be defined (likelihood levels in the risk rating methodology);
c) The timeframes of the likelihood and/or consequences;
d) How the level of risk is to be determined (risk rating);
e) The views of stakeholder;
f) The level at which risk becomes acceptable or tolerable; and
g) Whether combinations of multiple risk should be taken into account (interdependency) and, if so, and which combinations should be considered.

7. Risk Identification

Risk identification is a deliberated and systematic effort to identify and document the municipality's key risk. The objective of risk identification is to understand what is at risk within the context of the municipality's explicit and implicit objectives and to generate a comprehensive inventory of risk based on the threat and events that might prevent, degrade, delay or enhance the achievement of the objectives. This necessitated the development of risk identification guidelines to ensure that municipalities manage risk effectively and efficiently.

8. The risk identification process

Comprehensive identification and recording of risks are critical, because a risk that is not identified at this stage may be excluded from further analysis. In order to manage risks effectively, a municipality has to know what risks they are faced with. The risk identification process should cover all risks, regardless of whether or not such risks are within the direct control of the municipality. The municipality should adopt a rigorous and on-going process of risk identification that also includes mechanisms to identify new and emerging risk timeously.

Risk identification should be inclusive, not overly rely on the inputs of new senior officials and should draw as much as possible on unbiased independent source, including the perspective of important stakeholders.

9. Risk workshops and interviews

Risk workshops and interviews are useful for identifying, filtering and screening risks but it is important that these judgment based techniques be supplemented by more robust and sophisticated methods where required, including quantitative techniques.

Risk identification should be strengthened by supplementing management's perceptions of risk, inter alia, with;

- Review of external and internal audit reports;
- Financial analyses;
- Historic data analysis
- Actual loss data;
- Interrogation of trends in key performance indicator;
- Benchmarking against peer group of quasi peer group;
- Market and sector information
- Scenario analyses; and
- Forecasting and stress testing

10. Focus points of risk identification

To ensure comprehensiveness of risk identification the municipality should identify risk factors through consideration both internal and external factor, through appropriate processes of:

Strategic risk identification

Strategic risk identification to identify risk emanating from the strategic choices made by the municipality, specifically with regard to whether such choices weaken or strengthen the municipality's ability to execute its Constitutional mandate:

- Strategic risk identification should precede the finalization of strategic choice to ensure that potential risk issues are factored into the decision making process for selecting the strategic options;
- Risk inherent to the selected strategic choice should be documented, assessed and managed through the normal functioning of the system of risk management; and
- Strategic risk should be formally reviewed concurrently with changes in strategy, or at least once a year to consider new and emerging risks.

Operational risk identification

Operational risk identification to identify risks concerned with the municipality's operations:

- Operational risk identification should seek to establish vulnerabilities introduced by employees, internal processes and system, contractors, regulatory authorities and external events;
- Operational risk identification should be an embedded continuous process to identify new and emerging risks and consider shifts in known risks through mechanisms such as management and committee meetings, environmental scanning, process reviews and the like; and
- Operational risk identification should be repeated when changes occur, or at least once a year, to identify new and emerging risks.

Project risk identification

Project risk identification to identify risks inherent to particular projects:

- Project risk should be identified for all major projects, covering the whole lifecycle of each project; and
- For long term projects, the project risk register should be reviewed on a regular basis, such as quarterly and annually to identify new and emerging risks.

Although some projects may be multi-year projects, it remains important to continuously identify emerging issues that have an impact on project objective – either positive or negative. This could include internal risks such as a change in valuable resources, and external implications such as national policy or legislative changes that may have an impact on the project outcomes.

11. How to performs risk identification

It is crucial to have knowledge of the institutional environment before commencing with risk identification process. It is also important to learn from both experience and experience of others when considering the risk to which a

Municipality may be exposed and the best strategy available for responding to those risks.

Risk identification starts with understanding the Municipal objectives, both implicit and explicit. The risk identification process must identify unwanted events, undesirable outcomes, emerging threats, as well as existing and emerging opportunities. By virtue of a municipality's existence, risk will always prevail whether the municipality has control or not.

When identification risks, it is also important to bear in mind that ''risk'' also has an opportunity component. This means that there should also be a deliberate attention to identifying potential opportunities that could be exploited to improve municipal performance. In identifying risks, consideration should be given to risk associated with not pursuing an opportunity, e.g. failure

To implement an IT system to collect municipal rates.

Risk identification exercise should not get bogged down in conceptual or theoretical detail. It should also not limit itself to a fixed list of the risk categories, although such a list may be helpful.

The following are key steps necessary to effectively identify risk from across municipality:

- Understand what to consider when identifying risks;
- Gather information from different source to identify risks;
- Apply risk identification tools and techniques;
- Documents the risks;
- Document the risk identification process; and
- Assess the effectiveness of the risk identification process.

12. Understanding what to consider when identifying risks

In order to develop a comprehensive list of risk, a systematic process should be used that starts with defining objectives and key success factors for their achievement. This can help provide confidence that the process of risk identification is complete and major issues have not been missed.

13. Gather information from different source to identify risk

Good quality information is important in identifying risks. The starting point for risk identification may be historical information about this or a similar municipality. Discussion with a wide range of stakeholder about historical, Current and evolving issues, data analysis, review of performance indicators, economic information, loss data, scenario planning and the like can produce important risk information.

Furthermore, processes used during strategic planning like Strength Weakness Opportunity and Threats (SWOT) Analysis, Political Economic Social Technology Environment and Legal.(PESTLE) Analysis and benchmarking will have revealed important risks and opportunities that should not be ignored, i.e. they should be included in the risk register.

Certain disciplines like IT, Strategic Management, Health and Safety, etc. already have in place-established risk identification methodologies as informed by their professional norms and standards. The risk identification process should recognize and utilize the outputs of these techniques in order not to ''re-invent the wheel.

14. Apply risk identification tools and techniques

A Municipality should apply a set of risk identification tools and techniques that are suited to its objectives and capabilities, and to the risk the Municipalities faces. Relevant and up-to-date information is important in identifying risks. This should include suitable background information where possible. People with appropriate knowledge should be involved in identifying risk.

Approaches used to identify risks could include the use of checklists, judgments based on experience and records, flow charts, brainstorming, system analysis scenario analysis, and system engineering techniques.

- The approach used will depend on the nature of the activity under review, type of risk, the Municipality context, and the purpose of the risk management exercise.
- Team-based brainstorming for example, where facilitated workshops are used, is a preferred approach as it encourages commitment, considers different perspectives and incorporate different experiences.
- Structured techniques such as flow charting, system design review, system analysis, Hazard and Operability (HAZOP) studies and operational modelling should be used where the potential consequences are catastrophic and the use of such intensive techniques are cost effective.
- Since risk workshop are used only for filtering and screening of possible risks, it is important that the workshop are supplemented by more sophisticated or structured techniques described above.
- For less clearly define situations, such as the identification of strategic risks, processes with a more general structure, such as 'what-if and scenario analysis could be used.
- Where resources available for risk identification and analysis are constrained, the structure and approach may have to be adapted to achieve efficient outcome within budget limitation. For example where

less time is available, a smaller number of key element may be considered a higher level, or checklist may be used.

15. Document the risk identification

The risk identified during the risk identification are typically documented in a risk register that includes (at this stage):

- Risk description;
- How and why the risk can happen (i.e. causes and Consequences); and
- The existing internal control that may reduce the likelihood or consequences of the risk.

It is essential when identifying a risk to consider the following four elements:

- Description /event – an occurrence or a particular set of circumstance;
- Causes – the factors that may contribute to a risk occurring or increases;
- The likelihood of a risk occurring; and
- Consequences – the outcome(s) or impact (s) of an event.

It is the combination of these elements that make up a risk and this level of detail will enable a Municipality to better understand its risks.

16. Documents your risk identification process

In addition to documenting identified risks, it is also necessary to document the risk identification process to help guide future risk identification exercises and to ensure good practices are maintained by drawing on lessons learned through previous exercise.

Documentation of this step should include:

- The approach or method used for identifying risks;
- The scope covered by the identification;
- The participants in the risk identification; and
- The information source consulted.

Experience has shown that management often disregard well-controlled risk when documenting the risk profile of the Municipality. It is stressed that a well-controlled risk must still be recorded in the risk profile of the Municipality. The reason for this logic is that the processes for identifying risks should ignore at this point any mitigating factors (these will be considered when the risk is being assessed).

17. The outputs of risk identification

The document in which the risk are recorded is known as the ''risk register '' and it is the main output of a risk identification exercise.

A risk register is a comprehensive record of all risks across the municipality or project depending on the purpose/context of the register. There is no single blueprint for the format of a risk register and municipalities have a great degree of flexibility regarding how they lay out their document.

The risk register serves three main purposes

- It is a source of information to report the key risk throughout the municipality, as well as the stakeholder.
- Management uses the risk register to focus their priority risk.
- It helps the auditors to focus their plans on the municipality's to risk.

Once the risk have been identified, assessed and rated, and existing controls have been assessed, and it is has been established that controls are inadequate,

a risk response strategy needs to be determined, i.e. an assessment, for example, of whether the risk is acceptable or whether it needs to be treated.

18. Risk analysis

Risk analysis is a fundamental component of the risk management process. It helps to guide the evaluation of risks by defining the key parameters of the risk and how these may impact on the achievements of municipality's objectives.

One of the key outcomes of the risk assessment process is determining levels of risk exposure for the municipality. In addition, the data and related information collected during the risk assessment process can be used to assist in guiding risk responses decision.

19. Risk Analysis Methods

Method used in analysing risk can be qualitative, semi qualitative or qualitative. The degree of detail required will depend upon the particular application, the available data, the potential risk and the decision-making needs of the municipality, of if prescribed by legislation

a) **Qualitative assessment:** defines consequence, likelihood and level of risk by significance level such as ''high'', ''medium'' and ''low'', may combine consequences and likelihood, and evaluate the resultant level of risk against qualitative criteria. In qualitative analysis there should be a clear explanation of all the terns employed and the basis for all criteria should be recorded

b) Semi quantitate methods: Use numerical rating scale for consequences and likelihood descriptions and combine them to produce a level of risk using a formula. Scale may be linear o logarithmic. Or have someone other relationship and the formulae used can also vary.

c) Quantitative analysis: estimates numerical, practical values for consequences and their probabilities, and produces values of the level of risk in specific quantitative units. Full quantitative analysis may not always be possible due to insufficient data or information and often, due to the nature of the risk, the effort required of quantitative analysis is not warranted.

Even where full quantification has been carried out, it must be remembered that the calculation are estimates and they must not be attributed a level of accuracy and precision that is beyond the accuracy of the data and methods employed.

20. Risk analysis techniques

ISO 31010 lists several tools for risk analysis, but the more common ones are summarized below:

a) Root Causes Analysis

The analysis of a major loss to prevent its reoccurrence is referred to as Rood Cause Analysis (RCA). It attempts to identify the root or original causes instead of dealing only with the immediately obvious symptoms. Corrective action many not always be entirely effective and continuous improvement may be required.

RCA is applied in various context with the following broad areas of usage:

I. Safety-based RCA: for accident investigations and occupational health and safety;

II. Failure analysis: in technological systems related to reliability and maintenance;

III. Production-based RCA: applied in the field of quality control in capital projects like the development of a new city bus service or road building;

IV. Process-based : focus on business processes;

V. System-based: developed as a combination of the previous areas to deal with complex systems with application in change management, risk management and systems analysis.

b) Cause-and-effect analysis

Cause-and-effective analysis identified possible cause of an undesirable event or problem and organise the contributory factors into broad categories so that all possible options can be considered. The information is organised in either a fishbone (also called Ishikawa) or sometimes a tree diagram, and can be used as follows:

I. Provides a structure pictorial display of a list of causes of a specific effect. The effect may be positive (an objective) or negative (a problem) depending on context.

II. Used consider all possible scenario and causes generated by a team of experts and allows consensus to be established as to the most likely causes.

III. It is most valuable at the beginning of an analysis to broaden thinking about possible cause that can be considered more formally late

IV. It allows for a structure way to identify root causes, and identified six group of root causes, namely:

- Materials, which include lack of stock or medicines, lack of funding;
- Machines, which includes lack of equipment, or poorly designed application programs;

- Method, which includes a lack of processes, or poorly designed processes;
- Manpower, which includes lack of staff or skills, management incompetence or high vacancy rates, poor ethical practices;
- Measurements, which includes lack of dashboards, real-time monitoring of risk or lack of detection control; and
- Mother Nature, which reflects on external risk or political interference.

c) Decision tree analysis

A decision tree represents decision alternatives and outcomes is a sequential manner, which takes account of uncertain outcomes. It is similar to an event tree in that it starts from an initiating event or an initial decision and models different pathways and outcomes as a result of events that may occur and different decision that may be made. It can be used as follows:

I.   In managing projects risk and to help select the best course of action where there is uncertain; and
II. For communicating decision.

d) Bow Tie Analysis

Bow tie analysis is a simple diagrammatic way of describing and analysis the links within a risk from causes to consequences. A bow Tie is similar to a fault tree analysis the causes of an event and an event tree analysing the consequences. It can be used as follows:

I.   The focus of the bow tie is on the barriers between the causes and risk, and the risk and consequences.
II.   Bow Ties show a range of possible causes and consequences.
III. Bow tie analysis is often easier to understand than fault and even trees, and is useful communication tool

21. Risk assessment

Risk assessment involved interrogating risks at two levels, namely at the inherent risk level and the residual risk level, using the same rating criteria for each assessment.

Inherent risk considers the ''worst case'' scenario. This involves considering the likelihood and impact of the risk in the absence of any management control interventions. This level of assessment provides a perspective of the consequences of the risk to the municipality in its unmanaged state.

The second tier of assessment concerns establishing the residual risk. Residual risk is the level of remaining after the mitigating influence of the existing control interventions is considered. Normally, management would introduce sufficient control to reduce the risk to within a pre-determined level, as informed by the optimal risk level. The residual risk is a critical indicator of whether the existing control are effective in reducing the risk to an acceptable level.

When risks are assessed for the fragmented risk maturity status, the risk are assessed on a simplistic basis, as either high medium or low. When risk management has **integrated** or **risk intelligence** status, risks are assessed on the basis of the likelihood of the risk occurring and the impact of its occurrence (Risk= Likelihood times impact).

When assessing risk for risk intelligence municipalities, additional risk criteria could be applied, such as the level of volatility of the risk (i.e. the rate at which the risk could change if not addressed and responded to). This will further facilitate decision-making regarding the urgency of addressing particular risk, i.e. including or excluding certain risks from a risk response strategy, depending on whether it will deteriorate of diminish over time.

The magnitude of the consequences of an event, should it occur, and the likelihood of the event and its associated consequences, should be assessed in the context of the effectiveness of the existing strategies and control.

Consequences and likelihood may be estimated using statistical assessment and calculations where no reliable or relevant past data is available, subjective

estimates may be made which reflect an individual's or Municipality's degree of belief that a particular event or outcome will occur.

When rating the **impact** it is important to consider factors such as:

a) The value of transaction that pass through the process;
b) The importance of the activity in terms of the entity achievement its objective;
c) The impact this may have on other process within the entity;
d) The geographically dispersion of operation;
e) Ethically climate and pressure on management to meet objectives;
f) Financial and economic condition – frequency of losses;
g) Competency, adequate and integrity of staff;
h) Management information – key measurable indicator; and
i) Degree of information being processed on computerised information systems.

Impact rating can be defined as:

Impact	Description
Catastrophic	Loss of ability to sustain ongoing operations. A situation that would cause a standalone business to cease operation.
Major	Signification impact on achievement of strategic objectives and targets relating to the IDP of the municipality.

Moderate	Disruption of normal operations with a limited effect on the achievement of strategic objective or targets relating to the IDP.
Minor	No material impact on achievement of the municipality's strategy or objectives.
Insignificant	Negligible impact.

Table 16: Inherent risk ratings

When rating the likelihood it is important to consider factors such as:-

a) Broad or vague legislative authority or regulations, missions, goals or objectives;
b) High degree of complexity
c) Administration of contracts or grants;
d) Liquidity of assets;
e) Major restructuring of the municipality;
f) Relationship with suppliers and consumers;
g) Life expectancy of the internal control area;
h) Appropriateness of centralisation;
i) Classified or sensitive material;
j) Potential for conflict of interest; and
k) Management responsive

The ratings can be define as:

Likelihood	Description
Almost certain	The risk is almost certain to occur more than once within the next 12 months. (Probability =100% p.a.)
Likely	The risk is almost certain to occur once within the next 12 months. (Probability= 50-100% p.a.)
Moderate	The risk could occur at least once in the next 2 – 10 years. (Probability = 10-50% p.a.)

| Unlikely | The risk could occur at least once in the next 10-100 years. |
| Rare | The risk will probably not occur, i.e. less than once in 100 years. (Probability=0-1% p.a.) |

Table 17: Likelihood ratings

The most relevant source of information and techniques should be used when analysing consequences and likelihood. Source of information should include:

a) Past records, both financial and operational;
b) Audit reports from both internal and external auditors ;
c) Current legislation;
d) Practice and relevant experience;
e) Relevant published literature;
f) Market research;
g) The results of public consultation;
h) Experiments and prototypes;
i) Economic, engineering or other models; and
j) Specialist and expect judgments

Techniques that can be utilise will include;

a) Structure interviews with expects in the area of interest;
b) Use of multi-disciplinary group of experts;
c) Individual evaluations using questionnaires; and
d) Use of models and simulations.

Risk assessment should be performed in accordance with approved rating criteria for both likelihood and impact, combine the two to determine the overall risk rating.

Almost certain	5	10	15	20	25
Likely	4	8	12	16	20
Moderate	3	6	9	12	15
Unlikely	2	4	6	8	10
Rare	1	2	3	4	5
Likelihood	Insignificant	Minor	Moderate	Major	Catastrophic
	Impact				

RISK RATING

The colour coding will then lead to risk rating, which is reflected below:

Extreme	
High	
Moderate	
Low	

Table 18: Heat map – risk rating

Based on the assessment, risks are classified by level to determine the appropriate level of response to those risk. Specific response are defined at the ''Risk Response'' Phase.

22. Identify and evaluate existing control effectiveness

Controls may reduce the likelihood of occurrence of a potential risk, the impact of such a risk, or both. Management then needs to assess the control effectiveness based on their understanding of the control environment currently in place. Residual risk will therefore inform management of the actual level of control effectiveness.

Control should be considered on the basis of:

a. Design effectiveness – is the control ''fit for theory i.e. is the control designed appropriately for the function for which it is intended; and

b. Operational effectiveness – does the control work, as practically intended.it is useful to involve staff an understanding of the control when them. Internal audit, business analysts and operational/financial management can all provide input into control identification and assessment.

A well-designed and implemented control can often mitigate of reduce more than one risk or type of risk. Once effectiveness has been assessed, the residual risk rating can be calculated. Control then need to be evaluated. The first step in the process of risk control evaluation is to determine the adequacy of an individual control. This adequacy can be determined by asking questions around the controls design intent and purpose, its communication, whether

performance parameters have been defined and whether the control requires continual maintenance.

The second step is to determine the effectiveness of the control, i.e. how well is it used, is the control available when required, is it used as intended, has it been checked/validated?

For each control identified the risk control effectiveness value of the control must be established and rated. This can be done using the generic table below:

Risk Control Effectiveness	Interpretation
Fully effective	Controls are well designed for the risk – Review and monitor existing control
Partially effective	Most control are designed adequately and operate effectively. Address control weakness or improve operational efficiency.
Ineffective	A number of controls are not being used as intended, or not designed to treat the root cause of the risk.
Totally ineffective	Significant weaknesses in control design, with many gaps. Redesign control with focus on detection control.
None	Inadequate design of control/no control in place to mitigate risk

Table 19: Effectiveness ratings

23. Reference to the maturity index

The risk maturity index provides some clarity on the risk assessment process for municipalities with different maturities, as seen in the table below:

Risk assessment	Fragmented	integrated	Risk intelligent

Measurement	Risk are measured in green, yellow and red	Risk are measured on a colour scale, and ranked with a consistent metric like likelihood and impact.	Quantitative probabilities and impacts are estimated, using range for uncertainly. Volatility of risk and the risk environment is taken into consideration in prioritising risk response strategies.
Aggregation	Risk are aggregated and only measured on the worst-case scenario, on ad hoc basis.	Risk are aggregated for key performance objective, business processes and/or risk universe categories	Quantified probabilities and impacts allows for easy aggregation of risks across different dimensions and at any level of confidence using statistics. One view of aggregated risk table is applied for combined Assurance purpose

Table 20: Risk assessment per risk maturity index

The risk assessment templates are therefore adjusted accordingly.

24. Assessing of risk – fragmented risk maturity

The risk assessment in a fragmented status allows for risk management on a simplistic basis, where risk are assessed and aligned with control processes. Risk management might even be performed by internal audit units. Effectiveness of control process are evaluated by internal and external auditors, and the criteria for assessing risk and control is very basic (high, medium and low). There is no ability to calculate the risk appetite, identify root cause for system failures. There is a very low correlation between key performance indicators and risk indicators. An example of such a risk register will have the following layout:

Elements of Operational register	Operational risk 1			Explanation
Operational objective	Financially sustainable municipality, well maintained assets			Obtained from the IDP
Risk description	Irregular expenditure			
Risk category	Financial			Financial, operational or compliance – risk categories under the risk identification module
Inherent risk rating	High	Medium	Low	Multiply likelihood and impact and rate risk according to the assessment scale
Risk response	Mitigation			Identify risk response – mitigate, avoid, accept or transfer

Control processes	Bid evaluation and adjudication processes.			Identify current processes in place
Control effectiveness	ineffective	Partially effective	Effective	Rate the effectiveness of risk
Residual risk	High	Medium	Low	Calculate the remaining risk
Action plan	Implement accountability controls Allocate budget towards establishing risk management/internal audit unit			
Responsibility official	Municipal Manager			
Due date				

Table 21: Operational risk register – fragmented status

25. Assessing of likelihood and consequence – integrated risk management

The risk assessment in integrated risk management allows for the identification of likelihood and impact of different risk, and the ability to intergrade risks between different functions or responsibilities. Risk appetite is calculated, and residual risk is measured against the risk appetite. The risk exposure is reported to the 4th and 5th line of assurance as a matter of routine. An example of such a risk register will have the following layout:

Elements of operational risk register	Operational risk 1	Explanation

Operational objective	Financially sustainable municipality	Obtained from the strategies plan
Risk description	Irregular expenditure	
Risk category	Financial	Financial, operational or compliance, etc.
Root causes- internal	Over-riding of financial controls no second line of assurance	Use the fishbone diagram to determine the potential root cause for the risk
Root causes- external	Political interference	Use the fishbone diagram to determine the potential root cause for the risk
Consequence	Cash flow pressure inability to borrow	Brainstorming the consequences should the risk materialise
Likelihood	5	Rate the likelihood of risk materialising on a level of 1-5
Impact	4	Rate the import if risk materialising on a level of 1-5
Inherent risk rating	20	Multiply likelihood and impact and rate risk according to the assessment scale
Risk responses	Mitigation	Identify risk response- mitigate, avoid, accept or transfer

Control processes	Bid evaluation/adjudication processes.	Identify current processes in place
Control effectiveness	Effective	Rate the effectiveness of the risk
Residual risk	9	Calculating the remaining risk
Risk appetite	Zero tolerance for irregular expenditure	Measure the residual risk against the risk appetite
Action plan	Implement accountability controls

Allocate budget towards establishing risk management | |
| Responsible official | Municipal Manager | |
| Due date | | |

Table 22: Operational risk register – integrated status

26. Assessing of likelihood and consequence – risk intelligence management

The risk assessment in a risk intelligent environment allows for the identification of likelihood and impact of different risks, and the ability to integrate risks between different functions or responsibilities. Risk appetite is calculated, and residual risk is measured against the risk appetite. The future risk exposure is measured and reported to the 4th and 5th line of assurance as a matter of routine. In addition the second line of assurance monitors risk exposure on an ongoing

preventative basis and inform management timely when a risk might materialise. An example of such a risk register will have the following layout:

Elements of operational risk register	Operational risk 1	Explanation
Operational objective	Financially sustainable	Obtained from strategic plan
Key performance indicator		
Risk description	Irregular expenditure	
Risk category	Financial	Financial, operational or compliance etc.
Root causes - internal	Over- riding of financial controls No second line of assurance	Use the fishbone diagram to determine the potential root cause for the risk
Root causes – external	Political interference	Use the fishbone diagram to determine the potential root cause of the risk
Consequence	Cash flow pressure inability to borrow	Brainstorm the consequences should the risk materialise
Likelihood	5	Rate the likelihood of risk materialising on a level of 1 - 5
Impact	4	Rate the impact if risk materialises on a level of 1 - 5
Inherent risk rating	20	Multiply likelihood and impact and rate risk

		according to the assessment scale
Risk Response	Mitigation	Identify risk response – mitigate, avoid or transfer
Control processes implemented by management	Bid evaluation/adjudication Processes.	Identify current processes in place
Ongoing monitoring by risk management	Residual risk > risk appetite, automated aggregation and reporting to management ,audit committee and internal audit	Ongoing monitoring by risk management
Control effectiveness	Effective	Rate the effectiveness of the risk. Combined assurance, inclusive of independent assurance by internal audit
Residual risk	9	Calculate the remaining risk
Risk appetite	Zero tolerance for irregular expenditure	Measure the residual risk against the risk appetite
Residual risk > risk appetite		Calculate the risk exposure
Continuous monitoring by management	Reported as a key risk indicator, measured against the key performance indicator above	Preventative reporting – risk is reported to management before it actually materialise
Ongoing monitoring		

Action plan	Implement accountability controls Allocate budget towards establishing risk management	
Responsible official	Municipal Manager	
Due date		

Table 23: Operational risk register – risk intelligent status

27. Document risk assessment process

Documentation of the risk assessment process provide a record of how risk were analysed in previous periods, thereby informing future risk assessment exercises and providing constancy in how risk are identified, assessed and how decision are made regarding how risk are responded to. A key outcome of documenting the risk assessment process is enabling accurate tracking of risk over time using historical reference data.

Documentation should include

- Key assumption and limitation;
- Sources of information used;
- Explanation of the assessment method, and the definition of the term used to specify the likelihood and consequences of each risk;
- Existing control and their effectiveness;
- Description and severity of consequences;
- The likelihood of these specific occurrence; and resulting level of risk.

Detailed documentation may not be required for very low risks; however, a record should be kept of the rationale for initial screening of very low risk, for

example, in a volatile environment where risks of low security may change due to changing circumstance.

28. Risk assessment consideration

There are a number of other issues that must be considered in the context of risk assessment, which are noted below:

a. The risk assessment table need to be consistently applied for all key risk in the municipality.

b. Certain discipline, for example, IT and Health Safety, may utilise assessment methodologies that are informed by their professional norms and standards. In such circumstance, it would be prudent for the sake of the operational efficiency of these discipline to allow them to use their preferred methodology. However, in order to maintain consistency at the municipal level the same risks should be re-assessed in terms of the municipality-wide risk assessment methods.

c. The results of risk assessment could be represented in 'heat map'. These are a simple graphical representation of each risk according to the two scales, namely likelihood and impact.

d. Assessment of likelihood more often than not imposes a challenge to management. Guidance in this respect can be obtained from the historical experience of the municipality, as well as the experience of a similar municipality.

e. The assessments must be considered together with the municipality's risk appetite to determine whether the risk is acceptable or not. This in turn will inform whether additional intervention will be required.

29. Outputs

The output of risk assessment is a more sophisticated risk register which is enriched by the addition of ratings for each risk. This allows management to separate the more important risks from the less important ones and direct management attention accordingly.

30. Risk evaluation

The decision – making criteria should have been specified at the beginning of the risk management process and there may be other specific criteria mandated by legislation. Where risk are accepted 'as is' it is important to note any factors that may escalate them upwards, and hence require a response (consideration of the volatility of the risk and the risk environment). The decision about whether and how to treat the risk may depend on the costs and benefits of taking the risk and the costs and benefits of implementing improved controls.

Following evaluation, risk can be divided into five hands as can be seen in the table below:

Risk index	Risk magnitude	Risk acceptability	Action proposed
20 - 25		Unacceptable	Take action to reduce risk with highest priority
15 - 19			Take action to reduce risk – inform management
10 - 14			

5 - 9		Acceptable	Limited or no risk reduction, control and monitor, report to line manager
1 - 4			

Table 24: Risk index

31. Treat the risk – risk responses

A key outcome of the risk identification and assessment process is a detailed list if all key risk including those that require treatment as determined by the overall level of the risk against the municipality's risk tolerance levels. However, not all risks will require treatment as some may be accepted by the municipality and only require occasional monitoring throughout the period.

Although all key risk identified should be responded to, not all these risk will require treatment. The risk that fall outside of the municipality's risk tolerance level are those which pose significant potential impact on the ability of the municipality to achieve set objectives and therefore require treatment.

The purpose of risk responding to and treating risk is to minimize or eliminate the potential impact the risk may pose to the achievement of set objective.

Risk response is concerned with developing strategies to reduce or eliminate the threat and events that create risk. Risk response should also make provision for the exploitation of opportunities to improve the performance of the municipality. Responding to risk involves identifying and evaluating the range of possible option to mitigate risks and implementing the chosen option. Management should develop responses strategies for all material risks, whether

or not the management thereof is within the direct control of the municipality, prioritising the risk exceeding or nearing the appetite level.

Where the management of the risk is within the control of the municipality, the response strategies should consider:

a) Avoiding the risk by, for example, choosing a different strategy or termination the activity that produces the risk;
b) Treating the risk by, for example, implementing or improving the internal control system;
c) Transferring the risk to another party more competent to manage it by, for example, contracting out service, establishing strategic partnerships or buying insurance;
d) Accepting the risk where cost and strategy considerations rule out alternative strategies; and
e) Exploiting the risk factors by implementing strategies to take advantage of the opportunities presented by such risk factor. In instances where the management of risk is not within the control of the municipality, the response strategies should consider measures such as forward planning and lobbying. Response strategies should be documented an and the responsibilities and timelines attached thereto should be communicated to the relevant persons.

32.   Developing a risk response strategy

Risk response plans identify responsibilities, schedules, the expected outcome of responses, budget, performance measures and the review process to be set in place.

The risk response plans usually provide detail on:

a) Action to be taken and the risks they address;
b) Who has responsibility for implementing the plan;
c) What resource are to be utilized ;
d) The budget allocation;

e) The timetable for implementation ; and

f) Detailed of the mechanism and frequency of review of the status of the response plan.

33. **How to response to risk?**

Responding to risk involves the following key steps, each of which is covered in detailed in this section;

a) Identify risk responses;
b) Select risk response option;
c) Assign risk ownership;
d) Prepare risk response plans; and
e) Identify risk response options.

Identify risk response options

Risk response design should be based on a comprehensive understanding of how risks arise. This includes understanding not only the immediate causes of an event but also the underlying factor that influence whether the proposed response will be effective.

Risk response options are not necessarily mutually exclusive or appropriate in all circumstances. They should include the following:

a) Avoiding – not engaging in the activity that create risk exposure;
b) Mitigation risk – applying procedures that reduce the risk;
c) Transferring risk – transferring the risk exposure to other parties who may be better equipped or position to deal with it;
d) Exploiting risk – exploiting risk that represents an otherwise potential missed opportunity;

e) Accepting risk – accepting a risk with a low level of exposure;

f) Terminating risk – stopping the activity that gives rise to a risk higher than the acceptable level; and

g) Integrating some risks – applying some or all of the risk response to address a risk.

Select option for response

Once risk have assessed and a level of risk rating has been assigned, an option for response is selected. Consideration should be given to the cost of the response option as compared to likely risk reduction that will results.

For example, if the only available response option would cost in excess of R10m to implement and the cost impact of the risk is only R5m, it may not be advisable. It the risk volatility, however, is such that it may rapidly increase to exceed R10m, then this may become a viable decision.

In order to understand the cost and benefits associated with each risk response option, it is necessary to conduct a cost-benefit analysis.

Basis cost benefit analysis includes;

- Defining or breaking down the risk into its element by drawing up a flowcharts or list of inputs, output, activities and events;
- Calculate, researching or estimating the cost and benefit associated with each element. (include, if possible, direct, indirect, financial and social costs and benefits); and
- Comparing the sum of the costs with the sum of the benefits.

Assign risk ownership

The Municipal Manager allocate responsibilities for risk to an operational or functional area line manager.

Risk owner nominated by the Municipal Manager should assume responsibility for developing effective risk response plans. The risk owner (the person accountable for managing a particular risk) should be a manager with sufficient technical knowledge about the risk and/or risk for which a response is required.

The risk owner will often delegate responsibility (but not accountability) to his/her direct reports or consultants for detailed plan development and implementation. Once the option have been brainstormed and assessed, a risk treatment plan will be developed. This can be stand-alone plan, or additional columns on the risk register.

The process for developing the treatment plan is as follows:

a. Include the risk description and its risk rating in terms of consequence, likelihood and the overall rating.
b. List the treatment actions that were decided on following the risk treatment options discussion
c. Allocate a risk treatment owner who will take responsibility for the overall risk treatment.
d. Specific actions, i.e. the detailed steps.
e. Owners for the detailed actions or tasks need to be appointed
f. Resources that are required for achieving the tasks need to be determined, including financial, human and technical resources
g. The reporting requirements of progress with the completion of the task and actions need to be specified
h. Progress comments need to be made as part of the monitoring of the treatment action plan.

An example of a template is shown below:

Risk description:			Risk rating:			
Treatment action	Treatment owner	Action	Action owners	Resources needed	Reporting	Progress

Template 3: Treatment of risk

Prepare response plans

Once response option for individual risk have been selected, they should be consolidated into risk action plans and/or strategies.

As one risk response may impact on multiple risks, response actions for different risks need to be combined and compared so as to identify and resolve conflicts between plans and to reduce duplication of effort.

Response plans should:

- Identify responsibility, schedules, the expected outcome of responses, budgets, performance measure and the review process to be set in place include mechanisms for assessing and monitoring response effectiveness, within the context of individual responsibilities;
- Determine processes for monitoring response plan progress against critical implementation milestone aligned with the municipality's objectives. This information should all arise from response design process; and

- Document how the chosen option will be implemented practically.

The successful implementation of the risk response plan requires an effective management system that specifies the methods chosen, assigns responsibilities and individual accountabilities for actions, monitors them against specified criteria. Communication is a very important part of response plan implementation.

34. Opportunities versus threats

Measure both the downside and upside of risk-taking provides a context that can be used to determine the type and the amount of resources needed to support any project. Favourable outcomes, as projected by strategic planners and executive management, require a metric that is meaningful to the municipality. For example, the risk should be measured in terms of its impact on service delivery.

A benefit of measuring risk as a group is that as group is that analysing the range of possible outcomes against what was actually achieved may also provide executive management with insights into individual operational performance capabilities.

To be sure, the benefits of identifying and assessing both risk and opportunities at the same time might seem obvious, yet it is rarely practiced. One reason is that two widely used tools currently employed in Enterprise Risk management (ERM) risk assessment are the risk register and risk heat map. The focus of both of these is only the perceived threats to a municipality – they provide no consideration of the positive value that could be created by taking risks.

Risk register and risk maps have value under circumstances. Based on our research and analysis, we concluded that:

- If the municipal goal is to respond only to known and identified threats, and the ERM process is viewed as an extension of audit and compliance, risk register and risk heat maps can be useful.
- If the municipal goal is to respond to known threat and opportunities and gain risk intelligence about emerging perils on the horizon, traditional risk registers and risk heat maps fall short.
- If the municipal goal is to grow service delivery and create value for stakeholders traditional risk register and risk heat maps are useless.
- A new tool is required to measure both risk and opportunities. One example of such a tool is the Value Map – displayed below. Here both the threat and the opportunities are displayed.

A Sample Value Map

Outcome Likelihood	High probability										
	Low probability										
Negative Outcome							Positive Outcomes				
Outcome values											

Table 10: Sample value Map

A Value Map Is a graphical illustration of both threat and opportunities. Because threat and opportunities are two sides of the same coin. A value map also two sides, as illustrated above.   Threat (negativity outcome) are plotted on the left side of the map. While opportunities (positive outcome) are located on the right

side. Those outcomes value may be measures of successful service delivery or a project's net present value, for example.

The vertical axis shows the relative likelihood of an event happening. Rather than plotting a single point on a risk map, the value map illustrates the range of the magnitude of each situation.

The net value of threat(s) versus opportunity(s) could be determined, for example, for pursuing a particular municipal strategy.

Review of the Standard Operating Procedures

These procedures will be reviewed on an annual basis or when a need arises.

Process of monitoring and assessing risk response effectiveness

Risk monitoring is a process of keeping track of the identified risks, residual risks, and emerging risks. It also monitors the execution of planned strategies for the identified risks and evaluates their effectiveness and should be carried out as follows:

a) ERM shall monitor effectiveness of Risk Management and report outcomes to RMC thereof
b) Sharing of risk register that include risk responses and their target dates, to the directorates for their action
c) Monthly reviews of the highest probable and largest impact risk along with the mitigation strategies targeted for a month/quarter under review to enhance continuous improvement as follows:
   - Populating all risk and their targeted mitigation strategies of the financial year in a risk reporting template,

- Highlighting risk mitigation strategies that are due for reporting in the period under review including those not implemented in latter quarters,
- Mitigation strategies not implemented within a targeted timeframe should be carried over to the next review (noting that non implementation of mitigation strategies might translate to unconscious acceptance of the risk),
- Reports to ERM in a form of reporting template should be signed by the respective directors,
- Reviewed residual of a period under review should include residual of risks with mitigation strategies targeted for outer periods, for completeness in depicting the municipality's risk exposure,
- Indicate degree of implementation of mitigation strategies
- Indicate progress reported per mitigation strategy

d) Tracking a performance on KPIs as metrics of implemented mitigation strategies and or lack of implementation of mitigation strategies

e) Identification of and recording in a risk register all developments necessary and made to augment initial risk response or mitigation strategies.

Risk register template for risk profiling

Risk Ref.	Key Performance Areas	Strategic Objectives	Key Performance Indicator	Unit of measurement / output indicator	Risk Categories	Risks Description	Root Cause/ Contributing Factor	Consequence	Risk Assessment		Inherent risk	Current Controls	Risk Assessment After consideration of current controls			Future Action	Risk Owner	Due Date	Frequency of Reporting
									Impact	Likelihood	Total		Residual Impact	Residual likelihood	Total Residual Risk				

Monitoring and reporting tool (Risk evaluation template)

Risk Ref. and Risk Numbers	Contributing factors	Risk assessment			Current controls	Residual Risk rating (RIXRL) & movement of risks	Future/ Mitigating plans	Time frames on future plans	Progress up-to date	Reasons for missed timelines	Intervention	Comments by Risk Management Unit
		Inherent Impact	Inherent Likelihood	Total inherent risk rating								