

## **KWAZULU NATAL PROVINCIAL TREASURY**



# **RISK MANAGEMENT FRAMEWORK FOR MUNICIPALITIES AND MUNICIPAL ENTITIES**

*February 2011*

## CONTENTS

<b>1.</b>	<b>Foreword by the MEC of Finance .....</b>	<b>3</b>
<b>2.</b>	<b>Background.....</b>	<b>4</b>
2.1	Introduction.....	4
2.2	Overall purpose of the Enterprise Risk Management Policy and Framework.....	4
2.3	Key definitions.....	5
<b>3.</b>	<b>The purpose of the Enterprise Risk Management (ERM) Framework.....</b>	<b>6</b>
3.1	Purpose of the ERM framework.....	6
3.2	Benefits of the ERM policy and framework.....	6
3.3	Legal mandate.....	7
<b>4.</b>	<b>Risk Management Structures.....</b>	<b>10</b>
4.1	Introduction.....	10
4.2	Municipal Risk Management Oversight structure.....	10
4.3	Municipal Entities Risk Management Structures.....	12
<b>5.</b>	<b>Roles, responsibilities and governance .....</b>	<b>14</b>
5.1	Introduction.....	14
5.2	Members of Council .....	14
5.3	Accounting Officers (Municipal Manager / Chief Executive Officer).....	14
5.4	Risk Management Committee .....	15
5.5	Management .....	16
5.6	KwaZulu-Natal Provincial Treasury.....	17
5.7	Audit Committee .....	18
5.8	Fraud Prevention Committee .....	18
5.9	Departmental Heads.....	19
5.10	Chief Risk Officer (CRO).....	19
5.11	Internal Audit.....	20
5.12	The Auditor-General’s Office – External Audit .....	21
<b>6.</b>	<b>Enterprise Risk Management (ERM) Approach .....</b>	<b>22</b>
6.1	Introduction.....	22
6.2	Risk Profiles.....	22
6.3	Fraud Risk Assessment .....	24
6.4	Developing risk profiles .....	24
6.4.1	Risk Identification .....	24
6.4.2	Risk Categories.....	26
6.4.3	Risk Assessment.....	29
<b>7.</b>	<b>Communication and Reporting .....</b>	<b>37</b>
<b>8.</b>	<b>Combined Assurance .....</b>	<b>38</b>
<b>9.</b>	<b>Monitoring.....</b>	<b>39</b>
<b>10.</b>	<b>Embedding Risk Management .....</b>	<b>40</b>
	<b>Annexure A.....</b>	<b>41</b>
	<b>Annexure B.....</b>	<b>48</b>
	<b>Annexure C.....</b>	<b>52</b>
	<b>Annexure D.....</b>	<b>55</b>
	<b>Annexure E .....</b>	<b>56</b>
	<b>Annexure F .....</b>	<b>57</b>
	<b>Annexure G.....</b>	<b>58</b>

## 1. Foreword by the MEC of Finance

In the past, management of risk in the public service has not received adequate attention. With the introduction of the Municipal Finance Management Act (MFMA), Act 56 of 2003, the foundation has been laid for a more effective corporate governance framework as well as an accountable financial management system for the public sector. The Act has also established the legal framework for risk management in the public sector.

Today, more than ever, those in the public sector should be taking a long, hard look at risk – the threats to success and the possible consequences if they materialise. The importance of looking at risk comes in the wake of a more demanding society, bold initiatives and more challenge when things go wrong.

Public sector **risk management and control** should be firmly on the **agenda** for everyone involved in the public sector. Effective risk management processes will ultimately help achieve:

- **Greater organizational clarity of purpose** by clearly identifying policy needs and actions required to meet strategic objectives,
- **More cohesiveness of effort** through organizational consistency and clear role definition, **better decisions** through consideration of issues,
- **Faster reactions** through concentration on key performance trends, and
- **Accountability** by recording decisions in context and allocating responsibility for action.

Risk management processes and responsibilities are incorporated in the list of responsibilities allocated to Accounting Officers and Audit Committees. However, these responsibilities are extended to all Managers in terms of the provisions of the MFMA. The MFMA establishes responsibility for **Risk Management at all levels of management** and thus becomes everybody's responsibility. This should be seen as a medium term vision and to be successful it must assist in organisational and individual **behavioural change** and be seen to be of benefit to the individual as well as the organisation.

This risk management framework has been aligned to the Risk Management Frameworks issued by the National and Provincial Treasuries, to ensure a consistent approach to risk management at all levels of government in the Province. We therefore endorse the adoption of this risk management framework, by municipalities and municipal entities as a fundamental step towards an outward looking, accountable and innovative Public Sector.

Yours sincerely

---

MRS I. CRONJÉ, MP

MEC FOR FINANCE

DATE: \_\_\_\_\_

## 2. Background

### 2.1 Introduction

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

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

Public sector institutions are bound by constitutional mandates to provide products or services in the interest of the public good. As no institution has the luxury of functioning in a risk-free environment, public sector institutions also encounter risks inherent in producing and delivering such goods and services.

All institutions face uncertainty, and the challenge for management is to determine how much **uncertainty** the institution is prepared to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance **value**. The framework provides a basis for management to effectively deal with uncertainty of associated risk and opportunity, thereby enhancing its capacity to build value. Value is maximized when management sets objectives to strike an optimal balance between growth and related risks, and effectively deploys resources in pursuit of the institution's objectives. It is accordingly accepted by all stakeholders that municipalities and municipal entities will manage risks faced in an appropriate manner.

### 2.2 Overall purpose of the Enterprise Risk Management Policy and Framework

The **Enterprise Risk Management Policy** provides a framework within which management can operate to enforce the pro-active ERM process and to inculcate the risk management culture throughout the municipality and its municipal entities and to further ensure that the risk management efforts of the municipality and its municipal entities are optimised. It describes the municipality's and its municipal entities' ERM processes and sets out the requirements for management in generating risk management action, together with furthering risk management assurance. This document further sets out the municipality's policy on the management of risk at all levels of the organisation. A template risk management policy is included in Annexure B.

The **Enterprise Risk Management Framework** specifically addresses the structures, processes and standards implemented to manage risks on an enterprise-wide basis in a consistent manner.

Municipalities and municipal entities are not homogenous and therefore, this framework sets out the principles to support effective risk management. Institutions are expected to apply these principles in developing systems that are tailored to their specific environments. As the field of risk management is dynamic, this framework document is expected to change from time to time.

Current trends in good corporate governance, most notably the King Report on Corporate Governance (King III), have given special prominence to the process of ERM and reputable

organisations are required to demonstrate that they comply with expected risk management standards. This means that the municipality must ensure that the process of risk management receives special attention throughout the organisation and that ***all levels of management know, understand and comply with the framework document.***

## 2.3 Key definitions

### Risk

The Institute of Risk Management defines **risk** as “...***the uncertainty of an event occurring that could have an impact on the achievement of objectives.*** Risk not only manifests as negative impacts on the achievement of goals and objectives, but also as a missed opportunity to enhance organisational performance. Risk is measured in terms of consequences of impact and likelihood.”

This definition applies to each and every level of the enterprise and the overriding policy and philosophy is that the management of risk is the responsibility of management at each and every level in the municipality and its Entities. The management of risk is no more or less important than the management of organisational resources and opportunities and it simply forms an integral part of the process of managing those resources and opportunities.

### Enterprise Risk Management

Enterprise Risk Management (ERM) is the application of risk management throughout the institution rather than only in selected business areas or disciplines. ERM recognises that risks (including opportunities) are dynamic, often highly interdependent and ought not to be considered and managed in isolation. ERM responds to this challenge by providing a methodology for managing institution-wide risks in a comprehensive and integrated way.

ERM deals with risks and opportunities affecting value creation or preservation and is defined as follows with reference to COSO (The Committee of Sponsoring Organisations of the Treadway Commission):

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

The Public Sector Risk Management Framework guideline provided by the Office of the Accountant General at National Treasury defines risk management as “ a systematic process to identify, evaluate and address risks on a continuous basis before such risks can impact negatively on the institutions service delivery capacity. When properly executed risks management provides reasonable, but not absolute assurance, that the institution will be successful in achieving its goals and objectives.”

A full glossary of terms is included in Annexure A.

### 3. The purpose of the Enterprise Risk Management (ERM) Framework

#### 3.1 Purpose of the ERM framework

The purpose of the ERM framework is to provide a comprehensive approach to better integrate risk management into strategic decision-making; and

- Provide guidance for accounting officers, managers and staff when overseeing or implementing the development of processes, systems and techniques for managing risk, which are appropriate to the context of the municipality or municipal entity.
- Advance the development and implementation of modern management practices and to support innovation throughout the Public Sector;
- Contribute to building a risk-smart workforce and environment that allows for innovation and responsible risk-taking while ensuring legitimate precautions are taken to protect the public interest, maintain public trust, and ensure due diligence;

It is anticipated that the implementation of the Enterprise Risk Management Framework will:

- Support municipalities' governance responsibilities by ensuring that significant risk areas associated with policies, plans, programs and operations are identified and assessed, and that appropriate measures are in place to address unfavourable impacts;
- Improve results through more informed decision-making, by ensuring that values, competencies, tools and the supportive environment form the foundation for innovation and responsible risk-taking, and by encouraging learning from experience;
- Strengthen accountability by demonstrating that levels of risk associated with policies, plans, programs and operations are explicitly understood and that investment in risk management measures and stakeholder interests are optimally balanced; and
- Enhance stewardship and transparency by strengthening public sector capacity to safeguard human resources, property and interests.

#### 3.2 Benefits of the ERM policy and framework

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

- **Aligning risk appetite and strategy** – A municipality's management considers their risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks.
- **Pursuing institutional objectives through transparent identification and management of acceptable risk** – There is a direct relationship between objectives, which are what an entity strives to achieve and the ERM components, which represent what is needed to achieve the objectives.
- **Providing an ability to prioritise the risk management activity** – Risk quantification techniques assist management in prioritising risks to ensure that resources and capital are focused on high priority risks faced by the entity.
- **Enhancing risk response decisions** – ERM provides the rigor for management to identify and select among alternative risk responses – risk avoidance, reduction, sharing, and acceptance.
- **Reducing operational surprises and losses** – The municipality gains enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses.

- **Identifying and managing multiple and cross-enterprise risks** – A municipality faces a myriad of risks affecting different parts of the entity and ERM facilitates effective response to the interrelated impacts, and integrated responses to multiple risks.
- **Seizing opportunities** – By considering a full range of potential events, management is positioned to identify and proactively realize opportunities.
- **Improving deployment of capital** – Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation.
- **Ensuring compliance with laws and regulations** – ERM helps ensure effective reporting and compliance with laws and regulations, and helps avoid damage to the entity's reputation and associated consequences.
- **Increasing probability of achieving objectives** – ERM assists management in achieving the organization's performance and profitability targets and prevents loss of resources. Controls and risk interventions will be chosen on the basis that they increase the likelihood that the municipality will fulfill its intentions to stakeholders.

### 3.3 Legal mandate

The Municipal Finance Management Act, 2003 has legislated key governance best practices.

#### 3.3.1 Accounting Officer/Authority

Section 62(1)(i) of the Municipal Finance Management Act, 2003 requires that:

*“The accounting officer of a municipality is responsible for managing the financial administration of the municipality, and must for this purpose take all reasonable steps to ensure –*

*I that the municipality has and maintains effective, efficient and transparent systems –*

*(i) of financial and risk management and internal control”*

Section 95(i) of the Municipal Finance Management Act, 2003, requires that:

*“The accounting officer of a municipal entity is responsible for managing the financial administration of the entity, and must for this purpose take all reasonable steps to ensure -*

*I that the entity has and maintains effective, efficient and transparent systems –*

*(i) of financial and risk management and internal control”*

#### 3.3.2 Management, other personnel, Chief Risk Officer and Risk Champions

The extension of general responsibilities in terms of section 78 of the Municipal Finance Management Act, 2003 to all senior managers and other officials implies that responsibility for risk management vests at all levels of management and that it is not limited to only the accounting officer and internal audit.

Similarly, the extension of general responsibilities in terms of section 105 of the Municipal Finance Management Act, 2003 to all other officials of municipal entities implies that responsibility for risk management vests at all levels of management and that it is not limited to only the accounting officer and internal audit.

### 3.3.3 Internal Auditors

Section 165(2)(a)(b)(iv) of the Municipal Finance Management Act, 2003 requires that:

*“(2) The internal audit of a municipality must –*

- (a) Prepare a risk based audit plan and an internal audit program for each financial year;*
- (b) Advise the accounting officer and report to the audit committee on the implementation of the internal audit plan and matter relating to:*
  - (iv) risk and risk management”.*

Section 2110 – Risk Management of the International Standards for the Professional Practice of Internal Auditing States:

*“The internal audit activity should assist the organisation by identifying and evaluating significant exposures to risk and contributing to the improvements of the risk management and control systems –*

- A1 - The internal audit activity should monitor and evaluate the effectiveness of the organisation’s risk management system.*
- A2 - The internal audit activity should evaluate risk exposures relating to the organisation’s governance, operations and information systems regarding the:*
  - Reliability and integrity of financial and operational information;*
  - Effectiveness and efficiency of operations;*
  - Safeguarding of assets; and*
  - Compliance with laws, regulations and contracts.*
- C1 - During consulting engagements, internal auditors should address risk consistent with the engagement’s objectives and be alert to the existence of other significant risks.*
- C2 - Internal auditors should incorporate knowledge of risks gained from consulting engagements into the process of identifying and evaluating significant risk exposures of the organisation.”*

### 3.3.4 Audit Committee

Section 166 (2) of the Municipal Finance Management Act, 2003 requires that:

*“(2) An audit committee is an independent advisory body which must –*

- (a) Advise the municipal council, the political office-bearers, the accounting officer and the management staff of the municipality, or the board of directors, the accounting officer and management staff of the municipal entity, on matters relating to –*
  - (ii) risk management”*

### 3.3.5 Enterprise Risk Management Framework Guidelines

The Enterprise Risk Management Framework ensures that key risks are identified, measured and managed. The Enterprise Risk Management Framework provides management with proven risk management tools that support their decision-making responsibilities and processes, together with managing risks (threats and opportunities), which impact on the objectives and key value drivers.

ERM is everyone’s responsibility and must be embedded into the everyday activities of the municipality. This implies that ERM must be part of every decision that is made, every objective that is set and every process that is designed. Detailed ERM responsibilities for key risk management role players are listed below.



### **3.3.6 Corporate governance guidelines**

Institutions are encouraged to adhere to the principles espoused in the King Report on Corporate Governance (King III). King III discusses the following principles, which have been incorporated in this framework:

- Responsibility for the governance of risk;
- The determination of risk tolerance;
- The establishment of a risk committee;
- The responsibility of management to design, implement and monitor the risk management plan;
- The performance on continuous risk assessments;
- The implementation of frameworks and methodologies;
- The implementation of appropriate risk responses by management;
- The implementation of continuous risk monitoring by management; and
- Assurance to be provided on the effectiveness of the risk management process.

Similarly, the principles of Batho Pele clearly articulate the need for prudent risk management to underpin government objectives. Batho Pele strives to instil a culture of accountability and caring by public servants. Further objectives of Batho Pele include supporting the government's governance responsibilities, improving results through more informed decision-making, strengthening accountability and enhancing stewardship and transparency, all of which resonate well with the principles of risk management.

### **3.3.7 Applicability of the framework**

The Risk Management Framework for Municipalities shall be applicable to all metro, district and local municipalities, including municipal entities. Each municipality and municipal entity shall have a policy statement which makes reference to this framework.

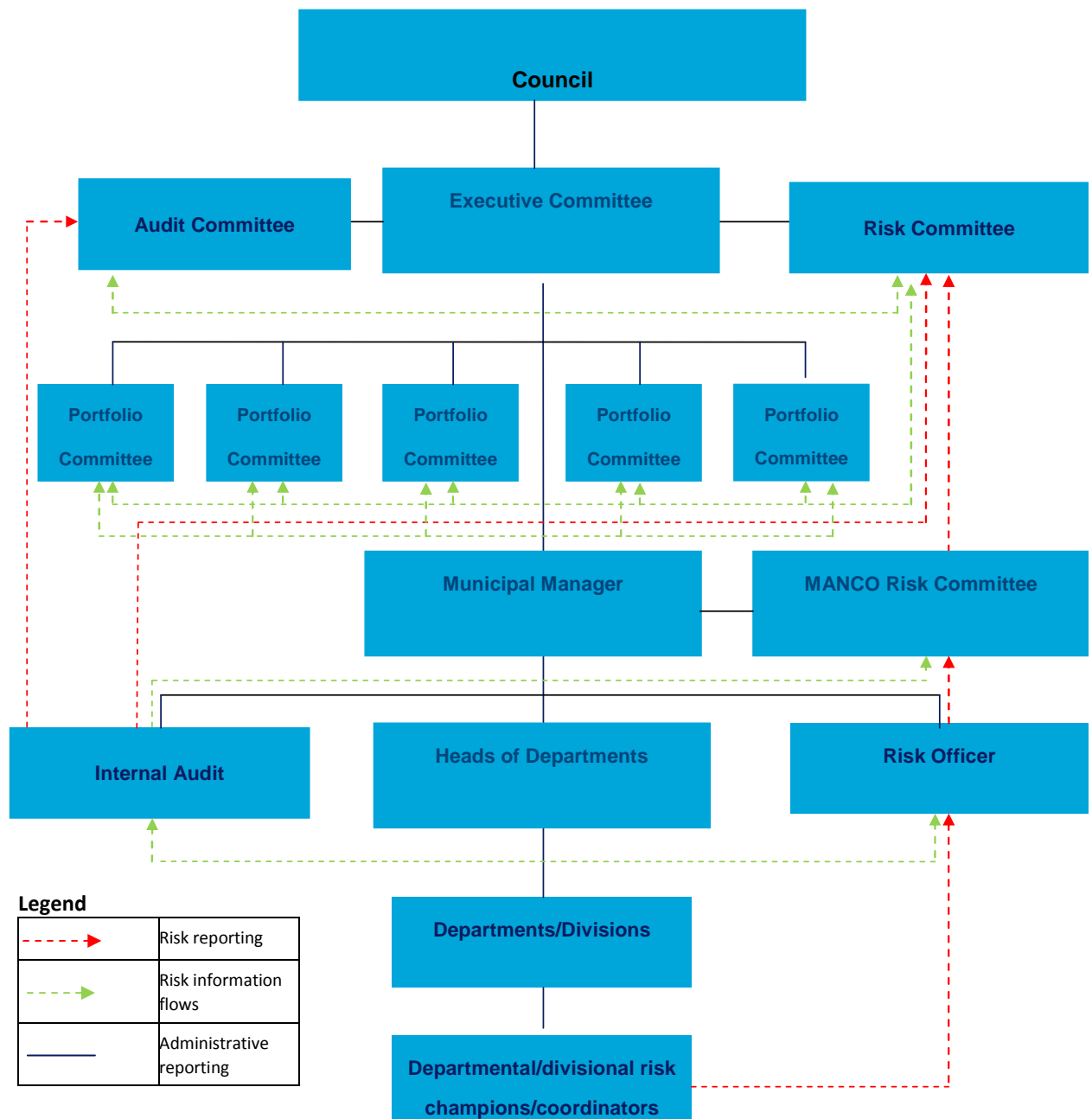
## 4. Risk Management Structures

### 4.1 Introduction

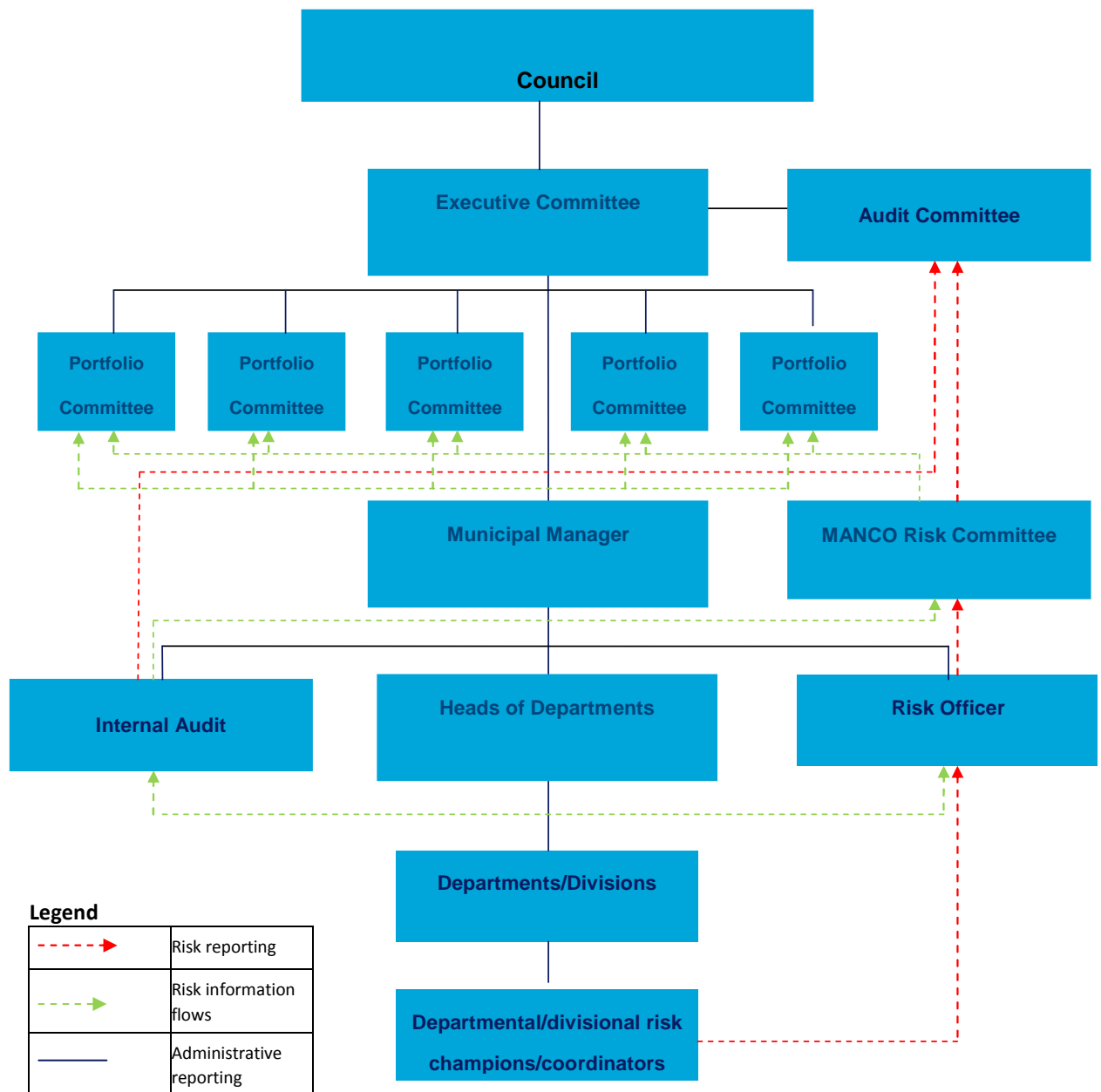
A risk management reporting and communication structure should be implemented to ensure oversight and accountability for enterprise risk management. The risk management structure should be tailored for the specific circumstances of each municipality or municipal entity. Example structures are included in the paragraphs below.

### 4.2 Municipal Risk Management Oversight structure

This structure would be applicable where you have constituted a separate Risk Management Oversight Committee with independent members (more relevant to high capacity municipalities):

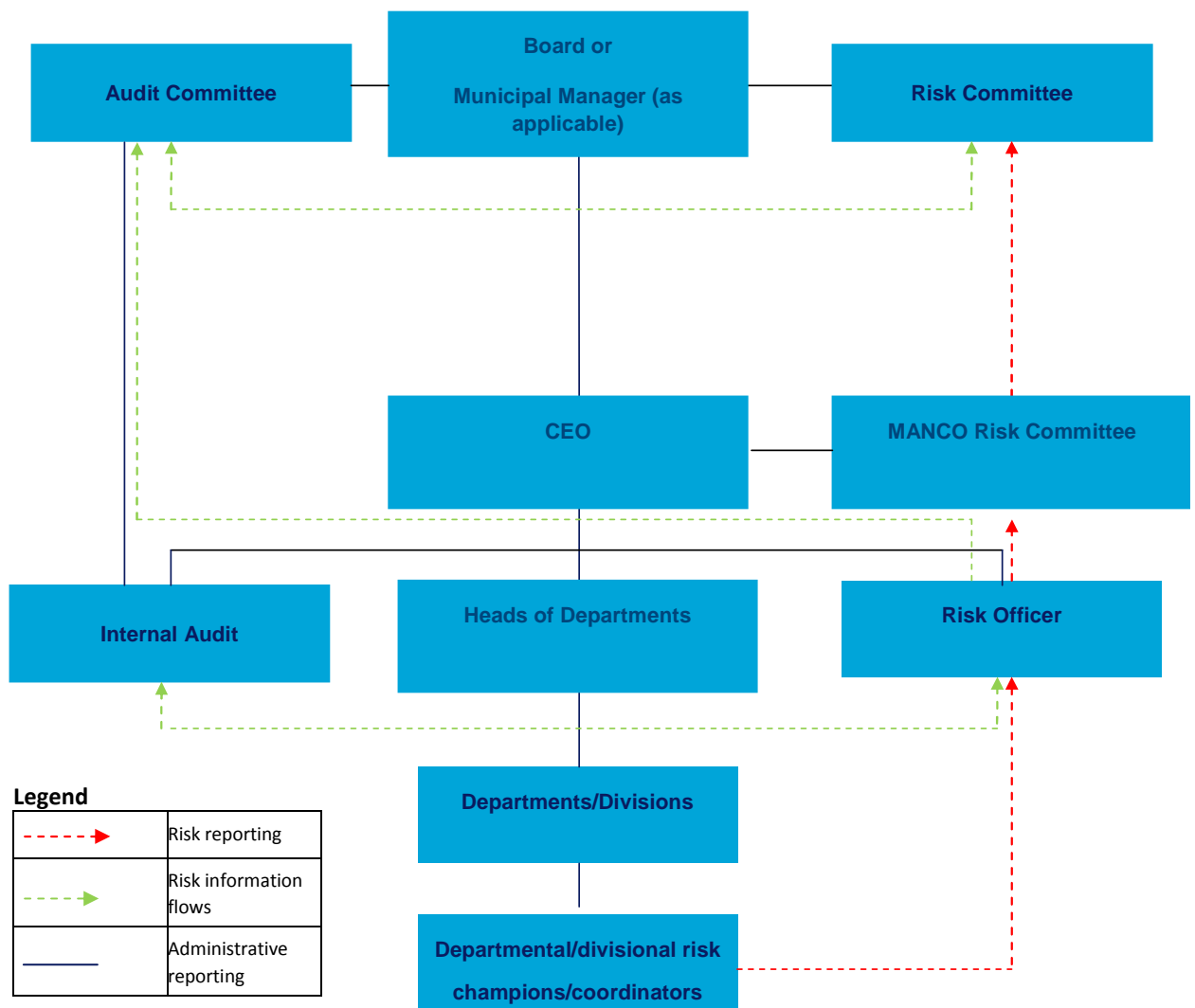


This structure would be applicable where you have constituted a MANCO Risk Committee reporting to the Audit Committee (more appropriate for smaller municipalities):

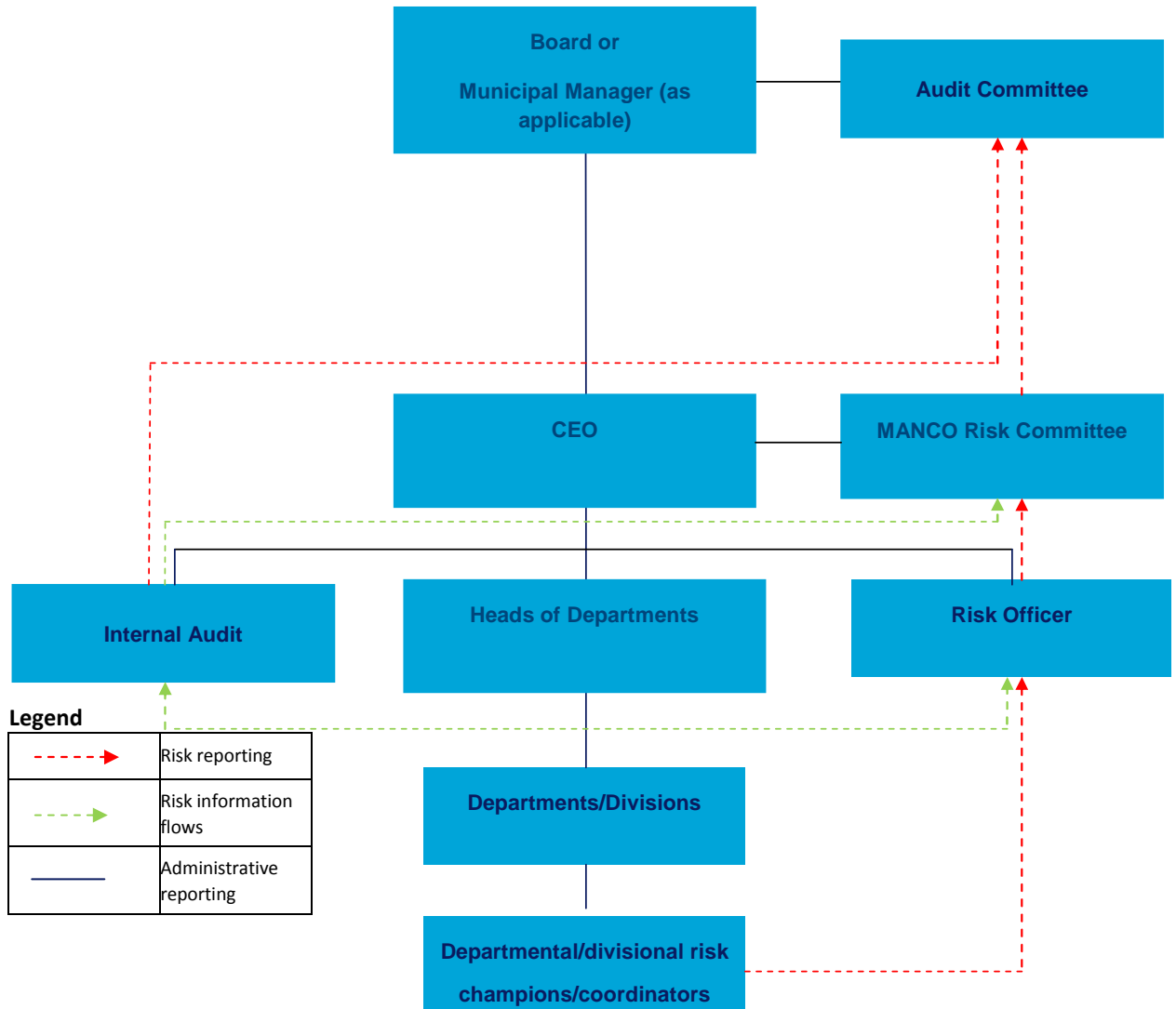


### 4.3 Municipal Entities Risk Management Structures

This structure would be applicable where you have constituted a separate Risk Management Oversight Committee with independent members (more relevant to high capacity municipal entities):



This structure would be applicable where you have constituted a MANCO Risk Committee reporting to the Audit Committee (more appropriate for smaller municipal entities):



## 5. Roles, responsibilities and governance

### 5.1 Introduction

- The Accounting Officer / Chief Executive Officer of each municipality or municipal entity is ultimately responsible for ERM and should assume overall ownership.
- All managers and employees have some responsibility for ERM.
- Managers support the risk management philosophy, promote compliance with the risk appetite and manage risks within their spheres of responsibility consistent with risk tolerances.
- Personnel are responsible for executing ERM in accordance with established directives and protocols.
- A number of external parties often provide information useful in effecting ERM, but they are not responsible for the effectiveness of the municipality's ERM processes and activities.

### 5.2 Members of Council

Councillors are collectively accountable for the achievement of the goals and objectives of the municipality and its municipal entities. As risk management is an important tool to support the achievement of this goal, it is important that the Councillors should provide leadership to governance and risk management.

Councils may delegate this responsibility to an Executive Committee of the Council.

High level responsibilities of the Council for their respective institutions for risk management include:

- Providing **oversight and direction** to the institution on the risk management related strategy and policies;
- Having knowledge of the extent to which the institution and management has established effective risk management in their respective institutions and **assign responsibility and authority**;
- Awareness of and concurring with the institution's **risk appetite and tolerance levels**;
- Reviewing the institution's **portfolio view of risks** and considering it against the risk tolerance;
- **Influencing** how **strategy and objectives** are established, institutional activities are structured, and risks are identified, assessed and acted upon;
- Requiring that management should have an established set of **values by which every employee should abide by**;
- Insist on the **achievement of objectives**, effective performance management, accountability and value for money.
- Consideration of:
  - The design and functioning of **control activities**, information and communication systems, and monitoring activities;
  - The quality and frequency of **reporting**;
  - The **way the institution is managed** including the type of risks accepted;
  - The appropriateness of the **reporting lines**.
- In addition the Council should:
  - Assign responsibility and authority;
  - Insist on accountability.

### 5.3 Accounting Officers (Municipal Manager / Chief Executive Officer)

The Accounting Officer (AO) is accountable for the institution's risk management in terms of legislation. It is important that the AO sets the right tone for risk management in the institution, this will ensure that the institution operates in a conducive control environment where the overall

attitude, awareness, and actions of management regarding internal controls and their importance to the institution is at par with the stated vision, values and culture of the institution.

Each AO/is responsible for:

- the **identification of key risks** facing their respective institution;
- the total process of risk management, which includes a related system of internal control;
- for forming its own opinion on the effectiveness of the process;
- providing **monitoring, guidance and direction** in respect of ERM;
- ascertaining the status of ERM within their respective institution, by discussion with senior management and providing **oversight** with regard to ERM by:
  - Knowing the extent to which management has established effective ERM;
  - Being aware of and concurring with the set risk appetite;
  - Reviewing the institution's portfolios view of risk and considering it against respective risk appetite; and
  - Considering the most significant risks and whether management is responding appropriately
- Identifying and fully appreciating the risk issues and key risk indicators affecting the ability of the institution to achieve its strategic purpose and objectives;
- ensuring that appropriate systems are implemented to manage the identified risks, by measuring the risks in terms of impact and probability, together with proactively managing the mitigating actions to ensure that the institutions assets and reputation are suitably protected;
- ensuring that the institutions ERM mechanisms provides an assessment of the most significant risks relative to strategy and objectives;
- considering input from the internal auditors, external auditors, auditor general, risk committee and subject matter advisors regarding ERM;
- utilising resources as needed to conduct special investigations and having open and unrestricted communications with internal auditors, external auditors, the auditor general and legal council;
- for disclosures in the annual report regarding ERM;
- Provide stakeholder's with assurance that key risks are properly identified, assessed, mitigated and monitored through receiving credible and accurate information regarding the risk management processes. The reports must provide an evaluation of the performance of risk management and internal control;
- Hold management accountable for designing, implementing, monitoring and integrating risk management principles into their day-to-day activities.

#### 5.4 Risk Management Committee

**The Risk Management Committee** is an oversight committee responsible to the Accounting Officer/Chief Executive Officer for the monitoring of risk management. It is responsible for assisting the Accounting Officer/Chief Executive Officer in addressing its oversight requirements of risk management and evaluating the institution's performance with regard to risk management. Management is accountable to the **Risk Management Committee** for **designing, implementing and monitoring** the process of risk management and **integrating it into the day-to-day activities** of the institution.

There is no legal mandate for the establishment of a Risk Management Committee. In terms of good governance, ideally a Risk Management Committee should be constituted of both independent members and management, and the chairperson of the Risk Management Committee should be an independent external person appointed by the Accounting Officer.

***However, given the situation faced by municipalities, it may be more practical for a MANCO Risk Committee be formed, with a reporting line to the Audit Committee to achieve oversight.***

The responsibilities of the Risk Committee may include:

- Review the risk management policy and strategy, and recommend for approval by the Accounting Officer;

- Review and assess the integrity of the risk control systems and ensure that the risk policies and strategies are effectively managed;
- Set out the nature, role, responsibility and authority of the risk management / risk officer function within the institution and outline the scope of risk management work;
- Monitor the management of significant risks to the institution, including emerging and prospective impacts;
- Review any legal matters, together with the legal advisor, that could have a significant impact on the institution;
- Review management and internal audit reports detailing the adequacy and overall effectiveness of the institution's risk management function and its implementation by management, and reports on internal control and any recommendations, and confirm that appropriate action has been taken;
- Review risk identification and assessment methodologies to obtain reasonable assurance of the completeness and accuracy of the risk register;
- Review and approve the risk tolerance for the institution;
- Evaluate the effectiveness of mitigating strategies to address the material risks of the Institution;
- Report to the Accounting Officer any material changes to the risk profile of the Institution;
- Review and approve any risk disclosures in the Annual Financial Statements;
- Monitor the reporting of risk by management with particular emphasis on significant risks or exposures and the appropriateness of the steps management has taken to reduce the risk to an acceptable level;
- Monitor progress on action plans developed as part of the risk management process;
- Review reports of significant incidents and major frauds (both potential and actual) including the evaluation of the effectiveness of the response in investigating any loss and preventing future occurrences;
- Significant incidents are defined as any event which results in, or has the potential to result in serious personal injury (to the public, staff or third parties) or serious physical damage to property, plant, equipment, fixtures or stock;
- Significant frauds are defined as any fraud which results in, or has the potential to result in the loss of assets with a value exceeding 10% of the institution' budget allocation;
- Providing feedback to the audit committee on the effectiveness of risk management;
- Develop goals, objectives and key performance indicators for the Committee for approval by the Accounting Officer;
- Develop goals, objectives and key performance indicators to measure the effectiveness of the risk management activity;
- Set out the nature, role, responsibility and authority of the risk management function within the Institution for approval by the Accounting Officer, and oversee the performance of the risk management function;
- Provide proper and timely reports to the Accounting Officer on the state of risk management, together with aspects requiring improvement accompanied by the Committee's recommendations to address such issues.

## 5.5 Management

Management is accountable to the Accounting Officer for designing, implementing and monitoring risk management, and integrating it into the day-to-day activities of the institution. This needs to be done in such a manner as to ensure that risk management becomes a valuable strategic management tool for underpinning the efficacy of service delivery and value for money.

Management is responsible for:

- designing an ERM programme in conjunction with the Chief Risk Officer;
- deciding on the manner in which risk mitigation will be embedded into management processes;
- ***inculcating a culture of risk management*** in the institution ;



- providing risk registers and risk management reports to the Chief Risk Officer pertaining to risk and control;
- identifying positive aspects of risk that could evolve into potential opportunities for the institution by viewing risk as an opportunity by applying the risk/reward principle in all decisions impacting upon the institution;
- assigning a manager to every key risk for appropriate mitigating action and determining an action date;
- holds official accountable for their specific risk management responsibilities;
- utilising available resources to compile, develop and implement plans, procedures and controls within the framework of the institution's Enterprise Risk Management Policy to effectively manage the risks within the institution;
- ensuring that adequate and cost effective risk management structures are in place;
- identifying, evaluating and measuring risks and where possible quantifying and linking each identified risk to key risk indicators;
- developing and implementing risk management plans including:
  - actions to optimise risk/ reward profile, maximise reward with risk contained within the approved risk appetite and tolerance limits;
  - implementation of cost effective preventative and contingent control measures
  - implementation of procedures to ensure adherence to legal and regulatory requirements;
  - monitoring of the ERM processes on both a detailed and macro basis by evaluating changes, or potential changes to risk profiles;
- implementing and maintaining adequate internal controls and monitoring the continued effectiveness thereof;
- implementing those measures as recommended by the internal auditors, external auditors and other assurance providers which, in their opinion, will enhance controls at a reasonable cost;
- reporting to the Audit Committee on the risk process and resultant risk/ reward profiles;
- defining the roles, responsibilities and accountabilities at senior management level.

## 5.6 KwaZulu-Natal Provincial Treasury

The MFMA makes it clear that Accounting Officers are responsible for implementing effective, efficient and transparent systems of risk management within the institutions under their control. Provincial Treasury (PT) must monitor that Municipalities comply in this regard. Furthermore, PT needs to assess the quality of implementation to ensure that implementation does not become the end of itself, but the means to help institutions to understand their risks and manage such risks in a prudent manner.

Section 5(4)(a)(i) of the MFMA, requires that PT monitor compliance with the Act by Municipalities in the Province.

Treasury's responsibilities include ***ensuring that all components of ERM are in place at all institutions***. Treasury generally fulfils this duty by:

- providing leadership and direction to the Accounting Officers. Together with the senior managers, Treasury shapes the values, principles and major operating policies that form the foundation of ERM processes at all levels of government in the Province. Key senior managers in the various institutions set strategic objectives, strategy and related high-level objectives.
- providing technical advice to the accounting officer and senior management on risk management strategies.
- reviewing and facilitating risk management training conducted at appropriate levels within the institutions to inculcate a risk management culture;
- analysing risk reports from various institutions and provide technical advice on the risk mitigation strategies.
- Assist institutions in facilitating risk assessments and developing risk mitigation strategies

Treasury has been appointed to provide direction, guidance, support, build capacity and to monitor institutions in effecting ERM.

## 5.7 Audit Committee

The Audit Committee is responsible for providing the Accounting Officer with independent counsel, advice and direction in respect of risk management. The stakeholders rely on the Audit Committee for an independent and objective view of the institution's risks and effectiveness of the risk management process. In this way, the Audit Committee provides valuable assurance that stakeholder interests are protected.

The Audit Committee oversees the roles and responsibilities of the Internal Audit team, specifically relating to providing assurance in respect of ERM.

The Audit Committee will be responsible for **addressing the governance requirements** of ERM and **monitoring the institution's performance with ERM activities**. The Audit Committee will meet quarterly and has a defined mandate and terms of reference, which covers the following aspects:

- constitution;
- membership;
- authority;
- terms of reference; and
- meetings.

The Audit Committee further:

- Reviews written reports furnished by the **Risk Management Committee detailing** the adequacy and overall effectiveness of the institutional Risk Committee's function and its implementation by management.
- Review risk philosophy, strategy, policies and processes recommended by the **Risk Management Committee and** consider reports by the **Risk Management Committee** on implementation and communication to ensure incorporation into the culture of the institutions.
- Ensure that risk definitions and contributing factors, together with risk policies, are formally reviewed on an annual basis.
- Review the acceptability of the risk profile in conjunction with the overall risk appetite of the institution, taking into account all risk mitigation factors, including, but not limited to, internal controls, business continuity and disaster recovery planning, etc.
- Ensure compliance with the risk policy and framework.
- Oversee the Fraud Prevention Committees of the institutions to ensure they are operating effectively and to receive periodic reports (quarterly) on their respective activities.
- Reviews the completeness of the risk assessment process implemented by management to ensure that all possible categories of risks, both internal and external to the institution, have been identified during the risk assessment process. This includes an awareness of emerging risks pertaining to the institution.
- Facilitates and monitors the coordination of all assurance activities implemented by the institution.
- Reviews and recommends any risk disclosures in the annual financial statements;
- Provides regular feedback to the Accounting Officer on the effectiveness of the risk management process implemented by the institution.
- Reviews and ensures that the internal audit plans are aligned to the risk profile of the institution.
- Reviews the effectiveness of the internal audit assurance activities and recommends appropriate action to address any shortcomings.

## 5.8 Fraud Prevention Committee

All institutions are obliged to appoint a Fraud Prevention Committee, to consist of members of staff drawn from a variety of levels of the institution. The Fraud Prevention Committee must ensure the implementation of the fraud and misconduct strategy, creating fraud awareness amongst all

stakeholders and accepting responsibility for considering any reports of fraud or misconduct and for taking appropriate action in consultation with the Head of institution.

The Head of institution establishes the right tone for the prevention and management of fraud and misconduct in the institution. This is achieved through developing and publishing a fraud and misconduct risk management policy.

The Fraud Prevention Committee, in fulfilling its role, is responsible for ensuring that the following is achieved:

- Monitoring of the **application of the policy** and ensuring adequate supervision and dynamism of the controls and procedures.
- The **planned and required activities are undertaken** such as the policy inclusion in the letter of appointment for staff, communication and training campaigns.
- Review the fraud prevention policy and recommend for approval by the Accounting Officer;
- Evaluate the effectiveness of the implementation of the fraud prevention policy;
- Reviews the process implemented by management in respect of fraud prevention and ensures that all fraud related incidents have been followed up appropriately.
- An appropriate **fraud risk assessment** is completed.
- The reports of fraud and misconduct are **effectively handled**.
- Consistent and **appropriate action** is taken on known incidents of fraud and misconduct.
- **Quarterly reports** to the Audit Committee that summarises the institution's fraud prevention, detection and action for the period.

## 5.9 Departmental Heads

Senior managers in charge of institutional departments have overall responsibility for managing risks related to their department's objectives and are responsible for:

- identifying, assessing and responding to risk relative to meeting the department's objectives;
- ensuring that the processes utilised are in compliance with the institution's Enterprise Risk Management policies and that their activities are within the established risk tolerance limits;
- reporting on progress and issues to the institutional Chief Risk Officer;
- complying with Enterprise Risk Management policies and developing techniques tailored to the department's activities;
- applying ERM techniques and methodologies to ensure risks are appropriately identified, assessed, responded to, reported on and monitored;
- ensuring risks are managed on a daily basis; and
- providing leadership with complete and accurate reports regarding the nature and extent of risks in the department's activities.

Institutions may have technical committees in place that deal with specialised areas of risk such as environmental management, quality management and technical compliance matters. These are expected to be continued as deemed appropriate for the risk profile of the institution.

## 5.10 Chief Risk Officer (CRO)

The primary responsibility of the CRO is to bring to bear his / her specialist expertise to assist the institution to embed and leverage the benefits of risk management to achieve its stated objectives. The CRO should be accountable to the Accounting Officer for enabling the business to balance risk and reward, and is responsible for coordinating the institution's ERM approach.

Note that in smaller institutions, it may not be feasible to appoint a CRO. In these circumstances, an existing position should be designated the responsibilities of the CRO, as described below.

The Chief Risk Officer:

- Working with senior management to develop the overall enterprise risk management vision, risk management strategy, risk management policy, as well as risk appetite and tolerance levels for approval by the Accounting Officer;
- undertakes a Gap Analysis of the institution's ERM process at regular intervals;
- performs reviews of the risk management process to improve the existing process;
- facilitates annual risk management assessments and risk assessments for all major changes and incidents, such as accidents, purchases of capital equipment, restructuring of operational processes etc.;
- develops systems to facilitate risk monitoring and risk improvement;
- ensures that all risk categories are included in the assessment;
- ensures that key risk indicators are included in the risk register;
- aligns the risk identification process with the institution's targets and objectives;
- agrees on a system of risk quantification;
- identifies relevant legal and regulatory compliance requirements;
- compiles a consolidated risk register on an annual basis;
- costs and quantifies actual non-compliance incidences and losses incurred and formally reports thereon;
- formally reviews the occupational health, safety and environmental policies and practices;
- consolidates all information pertaining to all risk related functions, processes and activities;
- reviews the Business Continuity Management Plans;
- liaises closely with the Internal Audit to develop a risk based audit plan and management assurance plans,
- benchmarks the performance of the risk management process to the risk management processes adopted by other entities both within South Africa and abroad;
- assists in compiling risk registers for all functional areas at strategic, tactical and operational levels;
- communicates the risk strategy to all management levels and to employees;
- ensures that the necessary risk management documentation is developed in respect of the risk management process;
- communicates with the Provincial Treasury, Audit Committee and the Risk Committee regarding the status of ERM;
- regularly visits functional areas and meets with senior managers to promote embedding risk management into the culture and daily activities of the institution;
- works with institutional leaders to ensure institutional plans and budgets include risk identification and management;
- Compiling the necessary reports to the Risk Management Committee;
- Providing input into the development and subsequent review of the fraud prevention strategy, business continuity plans, occupational health, safety and environmental policies and practices, and disaster management plans.

## 5.11 Internal Audit

Internal Audit is accountable to the Accounting Officer for providing independent assurance regarding the risk management activities of an institution. Hence, Internal Audit is responsible for providing independent assurance that management has identified the institution's risk and has responded effectively. Internal audit may also play an advisory and consulting role to Management regarding risk management matters.

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

- enhancing their understanding of risk management and the underlying concepts;
- assisting them to implement an effective risk management process, and
- providing objective feedback on the quality of organisational controls and performance."

**Internal Audit is responsible for:**

- Reviewing the risk philosophy of the institution. This includes the risk management policy, risk management strategy, fraud prevention plan, risk management reporting lines, the values that have been developed for the institution;
- Reviewing the appropriateness of the risk tolerance levels set by the institution taking into consideration the risk profile of the institution;
- Providing assurance over the design and functioning of the control environment, information and communication systems and the monitoring systems;
- Providing assurance over the institution's risk identification and assessment process;
- Utilising the results of the risk assessment to develop long term and current year internal audit plans;
- Providing independent assurance as to whether the risk management strategy, risk management implementation plan and fraud prevention plan have been effectively implemented within the institution;
- Providing independent assurance over the adequacy of the control environment. This includes providing assurance over the effectiveness of the internal controls implemented to mitigate the identified risks.

## **5.12 The Auditor-General's Office – External Audit**

In terms of the Public Audit Act, Number 25 of 2004, the Auditor-General is the Supreme Audit Institution (SAI) of South Africa, responsible for auditing financial statements of national government, provincial government and local government, and selected public entities.

The Auditor-General is responsible for providing an opinion on:

- The reasonability of the financial statements; and
- Compliance with applicable legislation

In addition, the Auditor-General is required to highlight weaknesses or deficiencies in the performance reporting of local government. In providing an opinion on compliance with legislation, the Auditor-General will provide independent assurance on the effectiveness of the risk management activities.

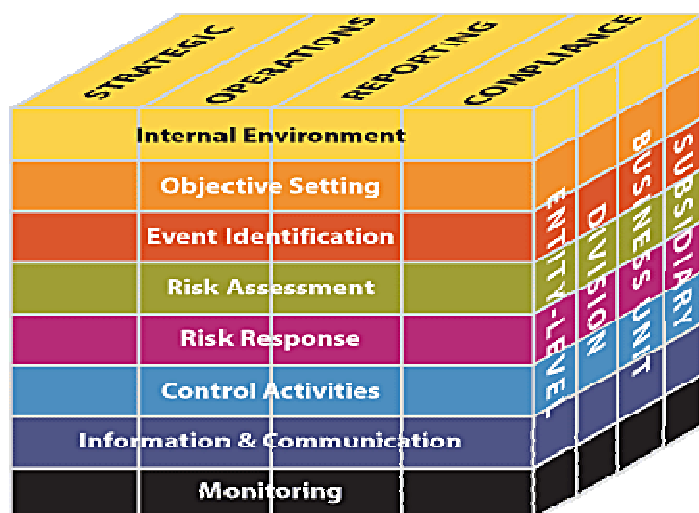
Within this mandate, the Auditor-General has undertaken to review and comment on the risk management practices within municipalities.

This framework therefore aims to assist the municipality in ensuring that the requirements of the Act are met through the application of effective risk management that is integrated with Internal Audit for the purposes of effective financial reporting and management of risk.

## 6. Enterprise Risk Management (ERM) Approach

### 6.1 Introduction

The ERM approach is based on the COSO Risk Management Framework depicted in the diagram below.

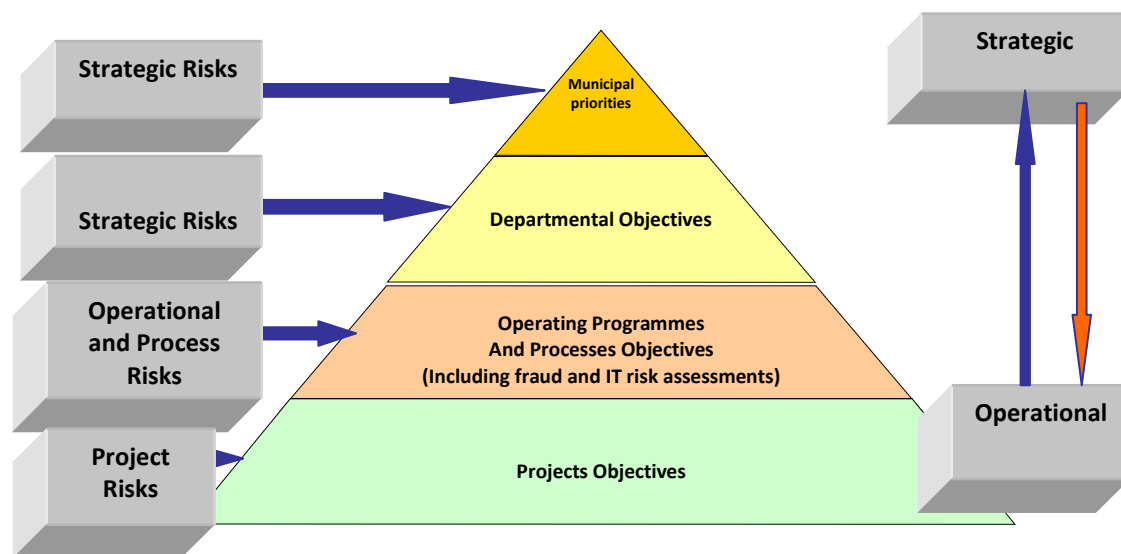


The implementation of enterprise-wide risk management is guided by the methodology outlined in this document. The methodology allows for a consistent approach to be applied by all municipalities and municipal entities in the Province and facilitates the interaction, on risk management matters, between the various institutions and functional areas within the institutions.

### 6.2 Risk Profiles

Risk profile plans shall be developed and reviewed on an annual basis. Four levels of risk profiles need to be developed and maintained at the institutions. These are:

- Strategic,
- Operational;
- Process; and
- Project.



The development and maintenance of the profiles should be a continuous process but management should formally assess and agree the profiles annually. This is usually achieved through facilitated workshops where management collectively agrees on the risk identification, assessment and actions.

#### **Strategic level**

- top-down risk assessments at strategic level should be performed when the vision, long-term development priorities and objectives are determined as part of the Integrated Development Plan;
- strategic risk identification should precede the finalisation of strategic choices, and related budgetary processes, to ensure that potential risk issues are factored into the decision making process for selecting the strategic options;
- in order to achieve this, the strategic risk assessment activities should be aligned to the activities in the IDP process plan and budget timetable and there should be a clear link between the challenges documented in the IDP and the key risks included in the strategic risk profile;
- strategic risk assessment should be updated during the annual review of the Integrated Development Plan and budgetary processes;
- in performing the strategic level risk assessment, risk owners assess the extent to which current management controls and strategies effectively mitigate identified risks to within the risk tolerance and overall risk appetite of the organisation;
- actions are implemented to respond to key gaps in risk mitigation, and monitoring of strategic risks, existing controls and actions should be integrated into day-to-day business.

#### **Operational level**

- operational risk identification should seek to establish vulnerabilities introduced by employees, internal processes and systems, contractors, regulatory authorities and external events;
- operational risk assessments should be performed during the annual departmental planning and budgeting processes, and be continually monitored for new and emerging risks;
- specific operational risk assessments may need to be performed in certain areas using specialist skills, such as fraud risk assessments (refer 6.3 below), information technology risk assessments, compliance risk assessments and safety and health risk assessments;
- in performing operational risk assessments, risk owners assess the extent to which current management controls and strategies effectively mitigate identified risks to within the risk tolerances;
- actions are implemented to respond to gaps in risk mitigation, and monitoring of operational risks, controls and actions should be integrated into operational day-to-day business.

#### ***Process level***

- process risk identification should seek to establish risks to the achievement of the specific process objectives;
- in performing process level risk assessments, risk owners assess the extent to which current management controls and strategies effectively mitigate identified risks to within the risk tolerances;
- actions are implemented to respond to gaps in risk mitigation, and monitoring of process level risks, controls and actions should be integrated into process level operations.

#### ***Project level***

- this involves the identification of risks inherent to particular projects;
- risks should be identified for all major projects, covering the whole project lifecycle;
- it is aimed to facilitate risk owners in ensuring that adequate and effective strategies and controls are implemented and monitored throughout the project lifecycle;
- risks documented in project risk register, monitored and regularly reviewed to identify new and emerging risks.

### **6.3 Fraud Risk Assessment**

A key element of the fraud and misconduct policy is the development of a fraud prevention plan. This plan is underpinned by a fraud risk assessment. The fraud risk assessment is completed according to the same process as the other risk assessments. However, an institution may wish to integrate the fraud risk evaluation together with the other risk profiles or to separately complete a fraud risk assessment. The fraud risk information will need to be extracted in order to develop and maintain the fraud prevention plan.

### **6.4 Developing risk profiles**

#### **6.4.1 Risk Identification**

The risk identification is defined as “the process of determining what, where, when, why, and how something could happen”. Risk identification is a deliberate and systematic effort to identify and document the institution’s key risks.

Risks emanate from internal or external sources which affects implementation of strategy or achievement of objectives.

As part of risk identification, management recognises that uncertainties exist, but does not know when a risk may occur, or its outcome should it occur. Management initially considers a range of potential risks – affected by both internal and external factors – without necessarily focusing on whether the potential impact is positive or negative.

Potential risks range from the obvious to the obscure, and the potential effects from the significant to the insignificant. But even potential risks with relatively remote possibility of occurrence should not be ignored at the risk identification stage if the potential impact on achieving an important objective is great.

The risk identification process should cover all risks, regardless of whether or not such risks are within the direct control of the institution. These might include external and internal factors:



<b>External Factors</b>	<b>Economic and Business</b>	Related risks might include emerging or movements in the international, national, provincial markets and globalisations
	<b>Natural environment</b>	Risks might include such natural disasters as flood, fire or earthquake, and sustainable development.
	<b>Political</b>	Risks might include newly elected government officials, political agendas and new legislation and regulations. The influence of international governments and other governing bodies
	<b>Social</b>	Risks might include changing demographics, shifting of family structures, work/life priorities, social trends and the level of citizen engagement
	<b>Technological</b>	Risks might include evolving electronic commerce, expanded availability of data and reductions in infrastructure costs.

<b>Internal Factors</b>	<b>Infrastructure</b>	Risks might include unexpected repair costs, or equipment incapable of supporting production demand.
	<b>Human resource</b>	Risks might include increase in number of on-the-job accidents, increased human error or propensity for fraudulent behaviour.
	<b>Process</b>	Risks might include product quality deficiencies, unexpected downtime, or service delays.
	<b>Technology</b>	Risks might include inability to maintain adequate uptime, handle increased volumes, deliver requisite data integrity, or incorporate needed system modifications.
	<b>Governance and accountability frameworks</b>	Values and ethics, transparency, policies, procedures and processes

Risk identification should be strengthened by:

- (a) Review of internal and external audit reports;
- (b) Financial analyses;
- (c) Historic data analyses;
- (d) Actual loss data;
- (e) Interrogation of trends in performance data;
- (f) Benchmarking against peer groups;
- (g) Market and sector information;
- (h) Scenario analyses; and
- (i) Forecasting and stress testing

There are a number of techniques that can be used for risk identification. The following options have been identified that can be used to assist roleplayers in identification and recording of perceived risks.

<u>Technique</u>	<u>Advantages</u>	<u>Disadvantages</u>
<b>Individual Interview</b>	Ensures consistent drawing out of issues. Personal interaction can be useful in generating a better understanding of risks.	Takes up a considerable amount of time for both interviewer and interviewee. May miss significant risks unless a well-qualified interviewer is used.

<u>Technique</u>	<u>Advantages</u>	<u>Disadvantages</u>
<b>Workshops</b>	Generates a shared understanding and “ownership”. Promotes team working through a process of brainstorming.	Team dynamics may take over (e.g. risks not identified because the “boss” is present which inhibits discussion). Negativity amongst the team affects risk ranking.
<b>A Combination of the Above</b>	Risks from interviews can be discussed and agreed. New risks can be brought out in a team environment.	Takes up officers’ time and largely depends upon the skills of the interviewer / facilitator.
<b>Staff Surveys</b>	Consistent questions asked and documented responses. Can identify risks, evaluate them and capture action plans.	Could be a better use of resources or be seen as bureaucratic and generate little “buy-in” from teams. Could there be some collation / analysis issues when results received.
<b>Selected Groupings</b>	If senior managers are involved they should quickly identify key strategic risks and the process can help to generate corporate working.	Fairly cost effective but the opinion of those “already converted” or risk educated may be sought which may not adequately capture or address a holistic approach.

#### 6.4.2 Risk Categories

Potential risks are grouped into categories. By aggregating risks horizontally across an organisation and vertically within operating units, management develops an understanding of the interrelationships between risks, gaining enhanced information as a basis for risk assessment.

<b>RISK CATEGORIES</b>	<b>DEFINITION OF RISK CATEGORIES</b>
<b>1. Strategic and service delivery risks</b>	Risks arising from policy decisions or major decisions affecting national, provincial municipal and organisational priorities; Risks arising from senior-level decisions on priorities. Strategy and Business Intelligence failures. Risks that have an effect of hindering service delivery due to inefficient, ineffective and uneconomical use of resources. Risks related to not delivering the appropriate quality of services to the citizens.

RISK CATEGORIES	DEFINITION OF RISK CATEGORIES
<b>2. Intergovernmental and Interdepartmental Co-ordination Risks</b>	Risks emanating from the relationship between the spheres of government in National, Provincial and Local levels as well as between municipal departments, and are having the effect of impeding the attaining of objectives
<b>3. Governance, Compliance/ Regulatory and Reputational Risks</b>	<p>Values and ethics, transparency, policies, procedures and processes as well organisational structures.</p> <p>Compliance with legal requirements such as legislation, regulations, standards, codes of conduct/practice, contractual requirements and internal policies and procedures. This category also extends to compliance with additional 'rules' such as policies, procedures or expectations, which may be set by contracts or customers.</p> <p>The reputation risks exposures due to the conduct of the entity as a whole, the viability of product or service, or the conduct of employees or other individuals associated with the business.</p>
<b>4. Political Risks</b>	<p>Risks relating to newly elected government officials, political agendas and new legislation and regulations or amendments thereof. The influence of international governments and other governing bodies on the institutional strategy.</p> <p>Risks emanating from political factors and decisions that have an impact on the institution's mandate and operations. Possible factors to consider include:</p> <ul style="list-style-type: none"> <li>• Political unrest;</li> <li>• Local, Provincial and National elections; and</li> <li>• Changes in office bearers.</li> </ul>
<b>5. Economic Risks</b>	<p>Risks relating to emerging or movements in the international, national, provincial markets and globalisations</p> <p>Factors to consider include:</p> <ul style="list-style-type: none"> <li>• Inflation;</li> <li>• Foreign exchange fluctuations;</li> <li>• Interest rates; and</li> <li>• Pricing.</li> </ul>
<b>6. Environmental Risks</b>	Risks relating to natural disasters as flood, fire or earthquake, and sustainable development.
<b>7. Social Risks</b>	Risks relating to poverty alleviation, changing demographics, shifting of family structures, work/life priorities, social trends, unemployment and the level of citizen engagement.
<b>8. Infrastructure Risks</b>	Risks relating to infrastructure e.g. roads, buildings, etc.
<b>9. Financial Risks</b>	<p>Risks arising from spending on capital projects. Risks from failed resource bids and insufficient resources. Risks encompassing the entire scope of general financial management. Potential factors to consider include:</p> <ul style="list-style-type: none"> <li>• Cash flow adequacy and management thereof;</li> <li>• Financial losses;</li> <li>• Wasteful expenditure;</li> <li>• Budget allocations;</li> <li>• Financial statement integrity;</li> <li>• Revenue collection; and</li> <li>• Increasing operational expenditure.</li> </ul>
<b>10. Health and Safety/Security Risks</b>	<p>Risks arising from outbreak of diseases and pandemic.</p> <p>Risks that is associated with the safety and security of the</p>

RISK CATEGORIES	DEFINITION OF RISK CATEGORIES
	communities as well as the execution of institutional mandate. Security of networks, systems and information.
<b>11. Shareholder Risks</b>	Risks associated with shareholding interests that the institution has with its stakeholders. Risks that could have a systemic impact on the sector within which the public entity operates and/or on the economy and service delivery.
<b>12. Human Resources</b>	Risks associated with staff capacity in relation to: <ul style="list-style-type: none"> <li>• Integrity and honesty;</li> <li>• Recruitment;</li> <li>• Skills and competence;</li> <li>• Employee wellness;</li> <li>• Employee relations;</li> <li>• Retention;</li> <li>• Non-familiarity of staff with the set guidelines and procedures, and</li> <li>• Occupational health and safety</li> </ul>
<b>13. Technological and System Risks</b>	Risks associated with evolving electronic commerce, expanded availability of data and reductions in infrastructure costs. Failure of application system to meet user requirements. Absence of in-built control measures in the application system. Risks relating specifically to the institution's IT objectives, infrastructure requirement, etc. Possible considerations could include the following when identifying applicable risks: <ul style="list-style-type: none"> <li>• Security concerns;</li> <li>• Technology availability (uptime);</li> <li>• Applicability of IT infrastructure;</li> <li>• Integration / interface of the systems;</li> <li>• Effectiveness of technology; and</li> <li>• Obsolescence of technology.</li> </ul>
<b>14. Process/operational</b>	Ineffective and inefficient processes. Inadequate controls in the operational processes.
<b>15. Project risks</b>	Risks associated with not meeting project scope, costs, duration and deliverables
<b>16. Fraud and Corruption Risks</b>	These risks relate to illegal or improper acts by employees resulting in a loss of the institution's assets or resources.
<b>17. Cultural</b>	Risks relating to an institution's overall culture and control environment. The various factors related to organisational culture include: <ul style="list-style-type: none"> <li>• Communication channels and the effectiveness;</li> <li>• Cultural integration;</li> <li>• Entrenchment of ethics and values;</li> <li>• Goal alignment; and</li> <li>• Management style.</li> </ul>
<b>18. Disaster Recovery/Business Continuity</b>	Risks related to an institution's preparedness or absence thereto to disasters that could impact the normal functioning of the institution e.g. natural disasters, act of terrorism etc. This would lead to the disruption of processes and service delivery and could include the possible disruption of operations at the onset of a crisis to the resumption of critical activities. Factors to consider include: <ul style="list-style-type: none"> <li>• Disaster management procedures; and</li> <li>• Contingency planning.</li> </ul>

RISK CATEGORIES	DEFINITION OF RISK CATEGORIES
<b>19. Knowledge and information management</b>	Risks relating to an institution’s management of knowledge and information. In identifying the risks consider the following aspects related to knowledge management: <ul style="list-style-type: none"> <li>• Availability of information;</li> <li>• Stability of the information;</li> <li>• Integrity of information data;</li> <li>• Relevance of the information;</li> <li>• Retention; and</li> <li>• Safeguarding.</li> </ul>
<b>20. Litigation</b>	Risks that the institution might suffer losses due to litigation and lawsuits against it. Losses from litigation can possibly emanate from: <ul style="list-style-type: none"> <li>• Claims by employees, the public, service providers and other third party;</li> <li>• Failure by institution to exercise certain rights that are to its advantage.</li> </ul>
<b>21. Loss / theft of assets</b>	Risks that an institution might suffer losses due to either theft or loss of an asset of the institution.
<b>22. Material resources (Procurement risk)</b>	Risks relating to an institution’s material resources. Possible aspects to consider include: <ul style="list-style-type: none"> <li>• Availability of material;</li> <li>• Costs and means of acquiring / procuring resources; and</li> <li>• The wastage of material resources.</li> </ul>
<b>23. Third party performance</b>	Risks related to an institution’s dependence on the performance of a third party. Risk in this regard could be that there is the likelihood that a service provider might not perform according to the service level agreement entered into with an institution. Non performance could include: <ul style="list-style-type: none"> <li>• Outright failure to perform;</li> <li>• Not rendering the required service in time;</li> <li>• Not rendering the correct service; and</li> <li>• Inadequate / poor quality of performance.</li> </ul>
<b>24. Natural environment</b>	Risks relating to the institution’s natural environment and its impact on normal operations. Consider factors such as: <ul style="list-style-type: none"> <li>• Depletion of natural resources;</li> <li>• Environmental degradation;</li> <li>• Spillage; and</li> <li>• Pollution.</li> </ul>

#### 6.4.3 Risk Assessment

Identified risks are analysed in order to form a basis for determining how they should be managed. Risks are associated with related objectives that may be affected. Risks are assessed on both an inherent and a residual basis, and the assessment considers both risk likelihood and impact. A range of possible results may be associated with a potential event, and management needs to consider them together.

Risk assessment allows consideration of the extent to which potential events might have an impact on the achievement of objectives. It is about analysing and assigning ratings to the potential likelihood (frequency or probability) of an event occurring, and the potential consequence (impact or magnitude

of effect), if the event does occur. The level of risk is determined by considering the combined effect of the likelihood and impact.

External and internal factors influence which events may occur and to what extent the events will affect the achievement of objectives. In performing a risk assessment, management considers the mix of potential future events relevant to the organisation and its activities. There are three important principles for assessing risk:

- ensure that there is a clearly structured process in place;
- record the assessment of risk in a way which facilitates monitoring and the identification of risk priorities; and
- be clear about the difference between, inherent and residual risk.

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

### **Inherent and Residual Risk**

Inherent risk is the risk in the absence of any actions management might take or has taken to reduce either the risk's likelihood or impact. Should there be existing controls, these must not be taken into account when estimating the inherent risk value. Inherent risks are rated, assuming that there are no controls in place to mitigate the risk.

The existence of controls, depending on how adequate and effective they are, may influence the likelihood or impact of the risk. This means that risk likelihood or impact may be reduced. Residual risk is the risk that remains after taking into account the effect of any existing controls. Example: The risk of theft of a car may be rated high. But having an immobilizer may reduce the likelihood of the risk occurring. The risk of theft may therefore be reduced.

In assessing risk, management considers the impact of expected and unexpected potential events. Many events are routine and recurring, and they are already addressed in management programs and operating budgets. Others are unexpected, often having a low likelihood of occurrence but may have a significant potential impact. Unexpected events usually are responded to separately. However, uncertainty exists with respect to both expected and unexpected potential events, and each has the potential to affect strategy implementation and achievement of objectives. Accordingly, management assesses the risk of all potential events that are likely to have a significant impact on the achievement of objectives.

Risk assessment is applied first to inherent risks. Once risk controls and responses have been identified and/or developed, the residual risk is then determined.

### **Likelihood and Impact**

Likelihood represents the probability that a given event or risk will occur while impact represents the effect of the risk should it occur.

### **Control**

A control could be policies, procedures, laws, regulations or any action that would reduce the likelihood or impact of a risk. For example: an insurance policy and an alarm system will reduce the impact and likelihood of the risk of theft respectively. Therefore the insurance policy and alarm system are referred to as controls.

There are different categories of controls and these are explained later in this document.

### Step 1: Estimating likelihood and impact

Risk assessment is tricky because the process involves subjective thinking. The identification of risks is generally based on an individual's experience and knowledge of the business and operations. Since experience and knowledge are unique to each individual, it is important to get a wide range of individuals on the risk management team. Each identified risk must be rated in terms of likelihood and impact.

Some types of risk lend themselves to a numerical diagnosis – particularly financial risk. For other risks - for example reputational risk - a much more subjective view is all that is possible. In this sense risk assessment is more of an art than a science. The assessment should draw as much as possible on unbiased independent evidence; consider the perspectives of the whole range of stakeholders affected by the risk.

Likelihood measures the probability that the identified risk / threat will occur within a specified period of time (between 1 and 3 years) on the basis that management have no specific / focused controls in place to address the risk / threat. The likelihood of occurrence must be assessed for every identified risk. Estimates of risk likelihood often are determined using data from past observable events, which may provide a more objective basis than entirely subjective estimates. Internally generated data based on the institution's own experience may reflect less subjective personal bias and provide better results than data from external sources.

There are also more scientific and objective methods of determining the likelihood and impact of a risk. The following rating scales have been established for municipalities and municipal entities.

#### Measures of likelihood of occurrence

Table of likelihood parameters

Likelihood category	Category definition	Rating
Common	The risk is already occurring, or is likely to occur more than once within the next 12 months	0.90
Likely	The risk could easily occur, and is likely to occur at least once within the next 12 months	0.65
Moderate	There is an above average chance that the risk will occur at least once in the next three years	0.40
Unlikely	The risk occurs infrequently and is unlikely to occur within the next three years	0.20
Rare	The risk is conceivable but is only likely to occur in extreme circumstances	0.10

## Measures of Impact

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

Severity ranking	Continuity of service delivery	Safety & Environmental	Technical complexity	Financial	Achievement of objectives	Rating
Critical	Risk event will result in widespread and lengthy reduction in continuity of service delivery to stakeholders of greater than 48 hours	Major environmental damage Serious injury (permanent disability) or death of personnel or members of the public Major negative media coverage	Use of unproven technology for critical system / project components High level of technical interdependencies between system / project components	Significant cost overruns of >20% over budget (higher of income or expenditure budget)	Negative outcomes or missed opportunities that are of critical importance to the achievement of objectives	100
Major	Reduction in supply or disruption for a period ranging between 24 & 48 hours over a significant area	Significant injury of personnel or public Significant environmental damage Significant negative media coverage	Use of new technology not previously utilised by the institution for critical systems / project components	Major cost overruns of between 10 % & 20 % over budget (higher of income or expenditure budget)	Negative outcomes or missed opportunities that are likely to have a relatively substantial impact on the ability to meet objectives	70
Moderate	Reduction in supply or disruption for a period between 8 & 47 hours over a regional area	Lower level environmental, safety or health impacts Negative media coverage	Use of unproven or emerging technology for critical systems / project components	Moderate impact on budget (higher of income or expenditure budget)	Negative outcomes or missed opportunities that are likely to have a relatively moderate impact on the ability to meet objectives	50
Minor	Brief local inconvenience (work around possibly) Loss of an asset with minor impact on operations	Little environmental, safety or health impacts Limited negative media coverage	Use of unproven or emerging technology for systems / project components	Minor impact on budget (higher of income or expenditure budget)	Negative outcomes or missed opportunities that are likely to have a relatively low impact on the ability to meet objectives	30
Insignificant	No impact on business or core systems	No environmental, safety or health impacts and / or negative media coverage	Use of unproven or emerging technology for non-critical systems / project components	Insignificant financial loss	Negative outcomes or missed opportunities that are likely to have a relatively negligible impact on the ability to meet objectives	10

### Step 2: Risk Matrix

Inherent risk exposure is the risk to the institution in the absence of any actions management might take to alter either the risk's impact or likelihood. Inherent risk is the product of the impact of a risk and the probability of that risk occurring before the implementation of any direct controls. The score for inherent risk assists management and internal audit alike to establish relativity between all the risks / threats identified.



The ranking of risks in terms of inherent risk provides management with some perspective of priorities. This should assist in the allocation of capital and resources in the operations. Although the scales of quantification will produce an automated ranking of risks, management may choose to raise the profile of certain risks for other reasons.

The table below is to be used to assist management in quantifying the inherent risk of a particular risk (i.e. pre controls)

Inherent risk exposure	Risk index value
Critical	≥ 60
Major	≥ 35 < 60
Moderate	≥ 20 < 35
Minor	≥ 10 < 20
Insignificant	< 10

For example: A likelihood of 0.20 and impact of 100 would result in a risk index of 20 and this correlates to a low risk. In this way each combination of likelihood and impact can be mapped to a risk index. The risk index indicates the severity of the risk.

### Step 3: Determining the risk acceptance criteria by identifying what risks will not be tolerated

#### Risk appetite

It is not always efficient to manage risks to zero residual risk or very low residual threshold because of the time, cost and effort that will be required, and which could result in the cost / benefit dynamics to become skewed. On the other hand it is also poor management practice to accept risks which create unnecessary exposure for the institution.

Given the aforementioned dynamics it is important for the institution to make an informed decision on how much risk it accepts as part of normal management practice. A quantitative approach in determining risk appetite has been adopted, reflecting and balancing goals for growth, return and risk. Risk appetite is directly related to strategy. It is considered in strategy setting, where the desired return from a strategy should be aligned with the risk appetite. Different strategies will expose different risks. Enterprise risk management, applied in strategy setting, helps management select a strategy consistent with risk appetite.

Defining a risk as acceptable does not imply that the risk is insignificant. The assessment should take into account the degree of control over each risk; the cost impact, benefits and opportunities presented by the risk and the importance of the policy, project, function or activity.

Reasons for classifying a risk to be acceptable could include:

- the likelihood and impact of the risk could be so low that specific treatment is inappropriate
- the risk being such that no treatment is available
- the cost of the treatment being so excessive compared to the benefit that acceptance is the only option.

The typical steps involved in establishing and implementing risk tolerance are:

1. Complete an analysis of the institution's ability to physically and financially recover from a significant event (e.g. risk such as human influenza pandemic, inability to supply, credit crunch, etc.)

2. The above analysis will highlight the need and importance of contingency plans, financial, physical and human resources and the importance of controls. From the analysis determine the tolerance the institution can bear or accept.
3. Management determines the level of tolerance which should then be endorsed by the Accounting Officer.
4. The risk tolerance levels set by the institution will be reflected in the risk rating scales used to assess the risks.

#### **Step 4. Considering the Risk Response**

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

Management selects an approach or set of actions to align assessed risks with risk appetite, in the context of the strategy and objectives. Personnel identify and evaluate possible responses to risks, including avoiding, accepting, reducing and sharing risk.

Risk responses fall within the following categories:

- **Avoidance-** Action is taken to exit the activities giving rise to risk. Risk avoidance may involve ceasing a project / activity, avoiding high risk investments, changing the objective, or not accepting a pioneering technical solution.
- **Reduction** – Action is taken to reduce the risk likelihood or impact, or both. This may involve any of a myriad of everyday business decisions. e.g. buying a generator to ensure electricity supply to a hospital, monitoring budgets / forecasts, defining accountability, improving staff morale, ensuring adequate skill sets.
- **Sharing** – Action is taken to reduce risk likelihood or impact by transferring or otherwise sharing a portion of the risk. Common risk-sharing techniques include purchasing insurance products, pooling risks, engaging in hedging transactions, or outsourcing an activity, public private partnership. e.g. taking out forward cover for foreign currency purchases.
- **Acceptance** – No action is taken to reduce the likelihood or impact of a risk. E.g. not to factor earthquakes greater than 5 on the Richter Scale to bridge construction due to the rare/remote probability of any seismic activity in the geographical area.

The avoidance response suggests that either the cost of other responses would exceed the desired benefit, or no response option was identified that would reduce the impact and likelihood to an acceptable level. Reduction and sharing responses reduce residual risk to a level that is in line with the risk appetites, while an acceptance response suggests that inherent risk is already in line with risk appetites.

For many risks, appropriate response options are obvious and well accepted. For instance, a response option appropriate for the loss of computing availability is the development of a business continuity plan. For other risks, available options may not be readily apparent, requiring more extensive identification activities. For instance, response options relevant to mitigating the effect of global warming may require research on weather patterns and water availability.

In determining the appropriate responses, management should consider such things as:

- Evaluating the effectiveness of existing measures on reducing the risk to an acceptable level.

- Considering if there are other control measures that could be used to mitigate the risk more effectively. This is where benchmarks and leading practices are important. In the public sector there are many opportunities to benchmark and consider leading practices as applied in other government institutions, provincial departments or local authorities.
- Assessing the costs versus benefits of potential risk responses.

#### **Step 5. Evaluating Effect of Response on Residual and Desired Residual Risk**

Each risk is rated according to the inherent risk rating criteria. The effectiveness of the existing risk responses is assessed for these risks. This is done by rating the control effectiveness. A decision is then needed to determine if the risk is managed to the desired levels of risk appetite. This is an assessment of the current residual risk.

Controls are the management activities / policies / procedures / processes / functions / departments / physical controls that the institution and Management have put in place, and rely upon, to manage the strategic and significant risks. These actions may reduce the likelihood of occurrence of a potential risk, the impact of such a risk, or both. When selecting control activities management needs to consider how control activities are related to one another.

Management then needs to assess the control effectiveness based on their understanding of the control environment currently in place. At this stage of the process, the controls are un-audited, and rated according to management’s interpretation of control effectiveness.

The table below is to be used to assist management in quantifying the perceived and desired control effectiveness to mitigate or reduce the impact of specific risks.

The desired effectiveness of risk responses is determined where the desired risk exposure is not achieved with current risk responses. The desired effectiveness is measured on the same scale as the rating for current control effectiveness. This is the assessment of desired residual risk for each risk – sometimes referred to as risk tolerance. The sum of risk tolerances should measure risk appetite.

Residual risk is calculated by multiplying the inherent risk score by the rating scale for control effectiveness.

<b>Effectiveness category</b>	<b>Category definition</b>	<b>Rating</b>
Very good	Risk exposure is effectively controlled and managed	0.20
Good	Majority of risk exposure is effectively controlled and managed	0.40
Satisfactory	There is room for some improvement	0.65
Weak	Some of the risk exposure appears to be controlled, but there are major deficiencies	0.80
Unsatisfactory	Control measures are ineffective	0.90

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

The difference between assessed residual risk and desired residual risk is the residual risk gap. This represents the opportunity to improve risk responses and the achievement of objectives. The bigger the residual risk gap, the higher the action priority.

The ranking of risks in terms of residual risk gap provides management with some perspective of priorities, and should assist in the allocation of capital and resources in the institution.

The table below is to be used to assist management in quantifying the residual risk gap of a particular risk.

Residual risk exposure	Risk acceptability	Proposed actions	Factor	Monetary Quantification
Critical	Unacceptable	Take action to reduce risk with highest priority, accounting officer/chief executive officer and executive authority/accounting authority attention.	≥ 60	≥ 5% of Budget or Income
Major	Unacceptable	Take action to reduce risk with highest priority, accounting officer/chief executive officer and executive authority/accounting authority attention.	≥ 35 < 60	≥4% <5% of Budget or Income
Moderate	Unacceptable	Take action to reduce risk, inform senior management.	≥ 20 < 35	≥3% <4% of Budget or Income
Minor	Acceptable	No risk reduction - control, monitor, inform management.	≥ 10 < 20	≥ 2.5% <3% of Budget or Income
Insignificant	Acceptable	No risk reduction - control, monitor, inform management.	< 10	2% of budget or income

The application of the approach has been depicted in the example and diagram below.

Inherent risk impact	Inherent risk likelihood	Inherent risk exposure	Perceived Residual risk	Desired Residual risk	Residual risk gap
Ranking with effective mitigation strategies in place (very good perceived effectiveness rating)					
100	0.90	90	0.25	0.20	4.5
Ranking with ineffective mitigation strategies in place (weak perceived effectiveness rating)					
100	0.90	90	0.80	0.20	54

### Step 6 . Identifying Actions to Mitigate Risk Exposure

The residual risk gap identifies possible improvement opportunities.

Action steps should be identified for the risks where there are residual risk gaps. The actions should specify the responsibilities and due dates. Management should track to progress and completion of the actions.

TIMESCALE FOR ACTION		
Colour-code of risk	Timescale for action	Timescale for review
Green – insignificant	Action within 12 months or accept risk	Review controls within 12 months
Yellow – minor	Action within 6 months	Review within 9 months
Yellow – moderate	Action within 3 months	Review within 6 months
Red – major	Action within 1 month	Review within 3 months
Red – critical	Action immediately	Review within 1 month

## 7. Communication and Reporting

Like any other process, the success of risk management depends on the availability of reliable information and effective communication at various levels. Pertinent information should be identified, captured and communicated in a form and time frame that enable people to carry out their responsibilities.

Information is needed at all levels to identify, assess and respond to risks. The challenge for management is to process and refine large volumes of data into relevant and actionable information. Risk information is to be maintained on a risk management database by the Risk Officer. Line management will be responsible for ensuring that the risk information is complete, accurate and relevant. The database will allow the access to the risk officials and line management to execute the relevant functions.

The database structure is based on the institution risk profiles, as follows:

- Strategic
- Operational ( Including Fraud and Corruption and IT)
- Project specific (where there are such projects)

Additional assessments can be maintained – for example incident tracking and compliance assessments.

For each profile the following minimum information is to be maintained on the database:

- Strategic and business objectives
- Risk category
- Risk name
- Risk description (including root cause and consequence)
- Risk owner
- Inherent risk rating
- Risk Indicator
- Control names for controls that mitigate the risk
- Control descriptions ( including whether it is a preventative, detective or corrective control)
- Control effectiveness rating
- Residual risk ratings
- Task information where identified – details, due dates and the accountable officials.
- Key Performance Indicator

The databases will be used to extract the required reports to evidence the status of risk management at the municipality.

## 8. Combined Assurance

Internal Audit is required by the MFMA to plan the audit coverage to address the risks identified through the risk management processes developed and maintained by management.

It is therefore imperative that the risk assessment process and the internal audit planning process be aligned so that timely and relevant risk information is available to internal audit when they are devising their audit coverage plans.

The risks identified cannot all be reviewed by Internal Audit. Some risks, for example reputation, are not able to be reviewed and others, such as technical construction, cannot reasonably be expected to be reviewed by Internal Audit.

There are several assurance functions that may exist in an institution at any time and include:

- The Office of the Auditor General,
- Internal Audit,
- Consulting engineers,
- Ethics' specialists,
- Compliance and Legal specialists,
- Culture and climate surveys,
- Health and safety inspectors,
- Information security,
- Quality,
- Loss Control Units, and
- Monitoring and evaluation Units

The assurance that they provide is reported to different management structures and this may be outside the Internal Audit governance reporting structures, including the Audit Committees.

Internal Audit takes the responsibility to ensure the assurance activities are coordinated, provide optimal coverage of the risk profiles, where possible, and are reported to the appropriate management and governance forum. The Audit Committee approves the overall/combined assurance plan and extent of assurance coverage. They will also review the appropriateness of the recipients of the different assurance activities.

Each assurance provider should develop their coverage plan based on the risk profiles of the institution(s). Typically the plan should consider the risk assessment ratings. Where management has assessed that there is a high residual risk gap and has actions to address the gap, the assurance provider should consider reviewing the actions rather than confirming management's assessment. Conversely where there is a low or negligible gap the controls that have been assessed by management as mitigating the risk should be evaluated.

The results of the work performed should be used by the chief risk officer to facilitate, if necessary, a re-rating of the risk and incorporating the agreed management actions into the risk management tasks. This will enable a central tracking capability for all such tasks and actions.

Where their work is in response to an incident or event, e.g. loss control, the results of the work performed should be used by the chief risk officer to facilitate, if necessary, a re-rating of the risk and incorporating the agreed management actions into the risk management tasks.

## 9. Monitoring

If existing controls are weak and exposes the organisation's activities to risks, the management should come up with the action plans to reduce risk to an acceptable level. Management should decide on the implementation date of the agreed upon action plan and the responsibility for the implementation of action plan should be assigned to capable officials.

It is critical that management should develop key performance indicators regarding the performance of agreed upon controls. Key performance indicators will provide the feedback regarding effectiveness of controls against identified risks.

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

- monitoring of progress made by management with the implementation of the ERM methodology;
- monitoring of key risk indicators;
- monitoring of loss and incident data;
- management's progress made with risk mitigation action plans; and
- an annual quality assurance review of ERM performance.

## 10. Embedding Risk Management

Value is created, preserved or eroded by management decisions ranging from strategic planning to daily operations of the institution. Inherent in decisions is the recognition of risk and opportunity, requiring that management consider information about the internal and external environment deploys precious resources and appropriately adjusts institution activities to changing circumstances. For governmental institutions, value is realized when constituents recognize receipt of valued services at an acceptable cost. Risk management facilitates management's ability to both create sustainable value and communicate the value created to stakeholders.

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

- Aligning risk management with objectives at all levels of the institution;
- Introducing risk management components into existing strategic planning and operational practices;
- Communicating institutional directions on an acceptable level of risk;
- Including risk management as part of employees' performance appraisals and Business Units' annual operational plans; and
- Continuously improving control and accountability systems and processes to take into account risk management and its results.



## Annexure A

### Glossary of Terms

<b>BASIC TERMS</b>	<b>DEFINITION</b>
<b><u>General Terminology</u></b>	
<b>Risk</b>	<p>Combination of the <b>probability</b> of an <b>event</b> and its <b>consequence</b></p> <p>Note 1: Risk is a condition in which the possibility of loss exists</p> <p>Note 2: In some situations risk arises from the possibility of deviation from the expected outcome or event</p> <p>Note 3: Risk arises as much from failing to capture business opportunities when pursuing strategic and operational objectives as it does from a threat that something bad will happen.</p>
<b>Consequence or Impact or Severity</b>	<p>Outcome of an <b>event</b></p> <p>Note 1: There can be more than one consequence from one event</p> <p>Note 2: Consequences range from positive to negative. However, consequences are always negative for safety aspects</p> <p>Note 3: Consequences can be expressed qualitatively or quantitatively</p>
<b>Probability</b>	<p>Extent to which the <b>event</b> is likely to occur</p> <p>Note 1: Frequency (the probability of an event occurring at intervals) rather than the probability (the relative likelihood of an event happening) may be used in describing risk</p> <p>Note 2: Degrees of believe about probability can be chosen as classes or ranks, such as rare/unlikely/moderate/likely/ almost certain, /improbable/remote/occasional/ probable/frequent</p>

<b>BASIC TERMS</b>	<b>DEFINITION</b>
<b>Event</b>	<p>Occurrence of a particular set of circumstances</p> <p>Note 1: The event can be certain or uncertain</p> <p>Note 2: The event can be a single occurrence or a series of occurrences</p> <p>Note 3: The <b>probability</b> associated with the event can be estimated for a given period of time.</p>
<b>Source/Cause</b>	Item or activity having a potential for a <b>consequence</b>
<b>Risk Criteria</b>	<p>Terms of reference by which the significance of <b>risk</b> is assessed</p> <p>Note : Risk criteria can include associated cost and benefits, legal and statutory requirements, socio economic and environmental aspects, the concern of stakeholders, priorities and other inputs to the assessment</p>
<b>Risk Management</b>	<p>Set of elements of an organisation's management system concerned with managing <b>risk</b></p> <p>Note 1: Management system elements can include strategic planning, decision making and other processes for dealing with risks</p> <p>Note 2: The culture of an organisation is reflected in its risk management system</p>
<b><u>Terms Related to People or Organisation Affected by Risk</u></b>	
<b>Stakeholder</b>	<p>Any individual, group or organisation that can affect, be affected by, or perceive itself to be affected by a <b>risk</b></p> <p>Note 1: The decision maker is also a stakeholder</p>

<b>BASIC TERMS</b>	<b>DEFINITION</b>
<b>Cost of risk</b>	Costs associated with: <ul style="list-style-type: none"> <li>• Insurance premiums</li> <li>• Self retained losses (incurred loss)</li> <li>• Loss control expenses including safety, security, property conservation, quality control programs, etc.</li> <li>• Administrative costs (internal and external) including risk management department, internal claims staff, fees paid to brokers, risk management consultants, outside claims and loss control services, including your time as risk manager and claims administrator</li> </ul>
<b>Interested Party</b>	Person or group having an interest in the performance or success of an organisation. Example: Customers, owners, people in an organisation, suppliers, bankers, unions, partners or society Regulators and Government are particularly interested in terms of the requirements of the Municipal Finance Management Act (MFMA).  The Accounting Officer's duties in terms of S62.1 of the MFMA (and other Acts / Regulations as amended from time to time) are specifically noteworthy.  Note : A group can comprise an organisation, a part thereof, or more than one organisation
<b>Risk Perception</b>	Way in which a stakeholder views a risk based on a set of values or concerns  Note 1: Risk perception depends on the <b>stakeholder's</b> needs, issues and knowledge  Note 2: Risk perception can differ from objective data
<b>Risk Communication</b>	Exchange or sharing of information about <b>risk</b> between the decision-maker and other <b>stakeholders</b>  Note : The information can relate to the existence, nature, form, probability, severity, acceptability, treatment or other aspects of risk

<b>BASIC TERMS</b>	<b>DEFINITION</b>
<b><u>Terms Related to Risk Assessment</u></b>	
<b>Risk Assessment</b>	<p>Overall process of <b>risk analysis</b> and <b>risk evaluation</b> in order to identify potential opportunities or minimise loss.</p> <p>Note: Risk assessment can be of a speculative nature (i.e. opportunity cost, poor operational efficiency, social impact on the municipality etc.) as well as pure perils (loss of assets, revenue etc.)</p>
<b>Risk Analysis</b>	<p>Systematic use of information to identify <b>sources</b> and to estimate the <b>risk</b></p> <p>Note1: Risk analysis provides a basis for <b>risk evaluation, risk treatment</b> and <b>risk acceptance</b>.</p> <p>Note 2: Information can include historical data, theoretical analysis, informed opinions, and the concerns of <b>stakeholders</b></p>
<b>Risk Identification</b>	<p>Process to find, list and characterise elements of <b>risk</b></p> <p>Note 1: Elements can include source or hazard, event, consequence and probability</p> <p>Note 2: Risk identification can also reflect the concerns of stakeholders</p>
<b>Source Identification</b>	<p>Process to find, list and characterise <b>sources</b></p> <p>Note : In the context of safety, source identification is called hazard identification</p>
<b>Risk Driver</b>	The technical, programmatic and supportability facets of risk.
<b>Risk Estimation</b>	<p>Process used to assign values to the <b>probability</b> and <b>consequences</b> of a <b>risk</b></p> <p>Note : Risk estimation can consider cost, benefits, the concerns of <b>stakeholders</b> and other variables, as appropriate for <b>risk evaluation</b></p>

<b>BASIC TERMS</b>	<b>DEFINITION</b>
<b>Risk Evaluation</b>	<p>Process of comparing the estimated <b>risk</b> against given <b>risk criteria</b> to determine the significance of the risk</p> <p>Note 1: Risk evaluation may be used to assist in the decision to accept or to treat a risk.</p>
<b><u>Terms Related to Risk Treatment and Control</u></b>	
<b>Risk Treatment</b>	<p>Process of selection and implementation of measures to modify <b>risk</b></p> <p>Note 1: The term “risk treatment” is sometimes used for the measures themselves</p> <p>Note 2: Risk treatment measures can include avoiding, optimising, transferring or retaining risk.</p>
<b>Risk Control</b>	<p>Actions implementing <b>risk management</b> decisions</p> <p>Note : Risk control may involve monitoring, re-evaluation, and compliance with decisions</p>
<b>Risk Optimisation</b>	<p>Process, related to a <b>risk</b> to minimise the negative and to maximise the positive <b>consequences</b> and their respective <b>probabilities</b></p> <p>Note 1: In the context of safety, risk optimisation is focused on reducing the risk.</p> <p>Note 2: Risk optimisation depends upon <b>risk criteria</b>, including costs and legal requirements.</p> <p>Note 3: Risks associated with <b>risk control</b> can be considered</p>
<b>Risk Reduction</b>	<p>Actions taken to lessen the <b>probability of</b> negative <b>consequences</b> or both, associated with a <b>risk</b></p>
<b>Mitigation</b>	<p>Limitation of any negative <b>consequence</b> of a particular <b>event</b></p>
<b>Risk Avoidance</b>	<p>Decision not to become involved in, or action to withdraw from, a risk situation</p> <p>Note: The decision may be taken based on the result of <b>risk evaluation</b></p>

<b>BASIC TERMS</b>	<b>DEFINITION</b>
<b>Risk Transfer</b>	<p>Sharing with another party the burden of loss or benefit of gain, for a <b>risk</b></p> <p>Note 1: Legal or statutory requirements can limit, prohibit or mandate the transfer of certain risk</p> <p>Note 2: Risk transfer can be carried out through insurance or other agreements</p> <p>Note 3: Risk transfer can create new risks or modify existing risk</p> <p>Note 4: Relocation of the <b>source</b> is not risk transfer</p>
<b>Risk Financing</b>	<p>Provision of funds to meet the cost of implementing <b>risk treatment</b> and related costs</p> <p>Note: In some industries, risk financing refers to funding only the financial consequences related to the <b>risk</b></p>
<b>Risk Retention</b>	<p>Acceptance of the burden of loss, or benefit of gain, from a particular <b>risk</b></p> <p>Note 1: Risk retention includes the acceptance of risks that have not been identified</p> <p>Note 2: Risk retention does not include treatments involving insurance, or transfer by other means.</p> <p>Note 3: There can be variability in the degree of acceptance and dependence on <b>risk criteria</b></p>
<b>Risk Acceptance</b>	<p>Decision to accept a <b>risk</b></p> <p>Note 1: The verb “to accept” is chosen to convey the idea that acceptance has its basic dictionary meaning</p> <p>Note 2: Risk acceptance depends on <b>risk criteria</b></p>
<b>Residual Risk</b>	The level of <b>Risk</b> remaining after <b>risk treatment</b>
<b>Inherent Risk</b>	The risk to an organisation in the absence of any management might take to alter either the risk probability or impact

<b>BASIC TERMS</b>	<b>DEFINITION</b>
<b>Chief Risk Officer (CRO) / Process Owner</b>	An official of the Municipality who has no <i>other</i> responsibilities except for advising on, formulating, overseeing and managing all aspects of an organisation's <b>risk management system</b> and monitors the organisation's entire risk profile, ensuring that major risks are identified and reported upwards. The CRO provides and maintains the risk management infrastructure to assist the council in fulfilling its responsibilities.
<b>Process Champion</b>	A senior executive within the Municipality who will lend support to the process and ensure senior managements buy-in. The risk process champion ensures that the <b>CRO</b> is provided with the necessary resources, capabilities and authority in order to fulfil the requirements of the Risk Management Framework.
<b>Risk Officers/Champions</b>	The risk officers assist the <b>CRO</b> in the fulfilment of their duties. These persons can be in line management in the departments but have an alternative reporting line to the <b>CRO</b> or report directly to the <b>CRO</b> .
<b>Risk Matrix</b>	The numbers of levels of probability and consequences chosen against which to measure risk.
<b>Risk Profile</b>	The Municipality has an <b>inherent</b> and <b>residual</b> risk profile. These are all the risks faced by the Municipality, ranked according to a <b>risk matrix</b> and indicated graphically on a matrix. The Risk Score is determined by multiplying the frequency and severity of the risk.
<b>Risk Appetite</b>	The level of <b>residual risk</b> that the organisation is prepared to accept without further <b>mitigation</b> action being put in place, or the amount of risk an organisation is willing to accept in pursuit of value  Note: An organisation's risk appetite will vary from risk to risk
<b>Risk Register</b>	A formal listing of risks identified, together with the results of the <b>risk analysis, risk evaluation</b> procedures together with details of <b>risk treatment, risk control, risk reduction</b> plans
<b>Key Risks</b>	Risks which the organisation perceives to be its most significant risks
<b>Key Risk Indicators</b>	Indicators by which key risks can be easily identified
<b>Risk Tracking</b>	The monitoring of key risks over time to determine whether the level of risk is changing.

## **Annexure B**

### **Template risk management policy**

#### **XXX Municipality**

#### **Enterprise Risk Management Policy**

### **1. POLICY STATEMENT**

The Accounting Officer has committed the XXX Municipality (Institution) to a process of risk management that is aligned to the principles of good corporate governance, as supported by the Municipal Finance Management Act (MFMA), Act no 56 of 2003.

Risk management is recognised as an integral part of responsible management and the Institution therefore adopts a comprehensive approach to the management of risk. The features of this process are outlined in the Institution's Risk Management Framework. It is expected that all departments / sections, operations and processes will be subject to the risk management framework. It is the intention that these departments / sections will work together in a consistent and integrated manner, with the overall objective of reducing risk, as far as reasonably practicable.

Effective risk management is imperative to the Institution to fulfil its mandate, the service delivery expectations of the public and the performance expectations within the Institution.

The realisation of our strategic plan depends on us being able to take calculated risks in a way that does not jeopardise the direct interests of stakeholders. Sound management of risk will enable us to anticipate and respond to changes in our service delivery environment, as well as take informed decisions under conditions of uncertainty.

We subscribe to the fundamental principles that all resources will be applied economically to ensure:

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

An entity-wide approach to risk management will be adopted by the Institution, which means that every key risk in each part of the Institution will be included in a structured and systematic process of risk management. It is expected that the risk management processes will become embedded into the Institution's systems and processes, ensuring that our responses to risk remain current and dynamic. All risk management efforts will be focused on supporting the Institution's objectives. Equally, they must ensure compliance with relevant legislation, and fulfill the expectations of employees, communities and other stakeholders in terms of corporate governance.



## 2. DEFINITIONS

### Risk

The Institute of Risk Management defines **risk** as “...*the uncertainty of an event occurring that could have an impact on the achievement of objectives*. Risk not only manifests as negative impacts on the achievement of goals and objectives, but also as a missed opportunity to enhance organisational performance. Risk is measured in terms of consequences of impact and likelihood.”

This definition applies to each and every level of the enterprise and the overriding policy and philosophy is that the management of risk is the responsibility of management at each and every level in the municipality and its Entities. The management of risk is no more or less important than the management of organisational resources and opportunities and it simply forms an integral part of the process of managing those resources and opportunities.

### Enterprise Risk Management

Enterprise Risk Management (ERM) is the application of risk management throughout the institution rather than only in selected business areas or disciplines. ERM recognises that risks (including opportunities) are dynamic, often highly interdependent and ought not to be considered and managed in isolation. ERM responds to this challenge by providing a methodology for managing institution-wide risks in a comprehensive and integrated way.

ERM deals with risks and opportunities affecting value creation or preservation and is defined as follows with reference to COSO (The Committee of Sponsoring Organisations of the Treadway Commission):

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

## 3. BENEFITS OF ENTERPRISE RISK MANAGEMENT

We expect the following benefits in adopting this enterprise risk management policy and effectively implementing the Enterprise Risk Management Framework:

- Aligning risk appetite and strategy
- Pursuing institutional objectives through transparent identification and management of acceptable risk
- Providing an ability to prioritise the risk management activity
- Enhancing risk response decisions
- Reducing operational surprises and losses
- Identifying and managing multiple and cross-enterprise risks.
- Seizing opportunities
- Improving deployment of capital

- Ensuring compliance with laws and regulations
- Increasing probability of achieving objectives

#### 4. ROLES AND RESPONSIBILITIES

The municipal risk management oversight structure is depicted below, with a summary of the specific responsibilities thereafter:

##### **Municipal Risk Management Oversight structure**

*Insert graphical representation of oversight structure tailored to the municipality*

##### **Members of Council**

Councillors are collectively accountable for the achievement of the goals and objectives of the municipality and its municipal entities. As risk management is an important tool to support the achievement of this goal, it is important that the Councillors should provide leadership to governance and risk management.

##### **Audit Committee**

The Audit Committee is responsible for providing the Accounting Officer with independent counsel, advice and direction in respect of risk management. The stakeholders rely on the Audit Committee for an independent and objective view of the institution's risks and effectiveness of the risk management process. In this way, the Audit Committee provides valuable assurance that stakeholder interests are protected.

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

The Risk Management Committee is an oversight committee responsible to the Accounting Officer/ Chief Executive Officer for the monitoring of risk management. It is responsible for assisting the Accounting Officer/Chief Executive Officer in addressing its oversight requirements of risk management and evaluating the institution's performance with regard to risk management.

##### **Accounting Officer (Municipal Manager / Chief Executive Officer)**

The Accounting Officer (AO) is accountable for the institution's risk management in terms of legislation. It is important that the AO sets the right tone for risk management in the institution, this will ensure that the institution operates in a conducive control environment where the overall attitude, awareness, and actions of management regarding internal controls and their importance to the institution is at par with the stated vision, values and culture of the institution.

##### **Management**

Management is accountable to the Accounting Officer for designing, implementing and monitoring risk management, and integrating it into the day-to-day activities of the institution. This needs to be done in such a manner as to ensure that risk management becomes a valuable strategic management tool for underpinning the efficacy of service delivery and value for money.

Senior managers in charge of institutional departments have overall responsibility for managing risks related to their department's objectives.

**Chief Risk Officer (CRO)**

The primary responsibility of the CRO is to bring to bear his / her specialist expertise to assist the institution to embed and leverage the benefits of risk management to achieve its stated objectives. The CRO is accountable to the Accounting Officer for enabling the business to balance risk and reward, and is responsible for coordinating the institution's ERM approach.

**Internal Audit**

Internal Audit is accountable to the Accounting Officer for providing independent assurance regarding the risk management activities of an institution. Hence, Internal Audit is responsible for providing independent assurance that management has identified the institution's risk and has responded effectively. Internal audit may also play an advisory and consulting role to Management regarding risk management matters.

**5. REVIEW OF POLICY**

The risk policy statement shall be reviewed annually to reflect the current stance on risk management.

**Every employee has a part to play in this important endeavor and we look forward to working with you in achieving these aims.**

Signed: \_\_\_\_\_

Accounting Officer: \_\_\_\_\_

Date: \_\_\_\_\_

## Annexure C

### Template [MANCO] risk committee terms of reference/charter

#### XXX Municipality

#### [MANCO] Risk Committee Terms of Reference

##### 1. Constitution

The [MANCO] Risk Committee (Committee) has been established by the XXX Municipality to assist the Municipal Manager to fulfil his risk management and control responsibilities in accordance with prescribed legislation and corporate governance principles.

##### 2. Objectives

The primary objective of the Committee is to assist the Municipal Manager in discharging his accountability for risk management by reviewing the effectiveness of the municipality's risk management systems, practices and procedures, and providing recommendations for improvement.

##### 3. Composition

Permanent members of the Committee shall be formally appointed by the Municipal Manager. The members, as a collective, shall possess the blend of skills, expertise and knowledge of the municipality, including familiarity with the concepts, principles and practice of risk management, such that they can contribute meaningfully to the advancement of risk management within the municipality.

Membership shall comprise [if Risk Committee]:

- Member of the Audit Committee,
- A member not in the employ of the municipality, and
- Representatives of senior management

Membership shall comprise [if MANCO risk committee]:

- Municipal Manager, and
- Heads of Department.

Standing invitees to the Committee shall be:

- Risk Officer;
- Head of Internal Audit;
- Compliance Officer;
- Any other person who may be co-opted to provide specialist skills, advice and counsel.

#### **4. Authority**

[If Risk Committee] The Municipal Manager shall appoint the Chairperson from the permanent membership of the Committee

[If MANCO risk Committee] The Municipal Manager shall be the Chairperson of the Committee.

The Committee shall have the requisite authority to request management to appear before it to account for their delegated responsibilities in respect of risk management.

#### **5. Roles and responsibilities**

The duties of the Committee shall be to:

- Review the risk management policy and strategy and recommend for approval by the Municipal Manager and Council;
- Review the risk appetite and tolerance and recommend for approval by the Municipal Manager and Council;
- Review the municipality's risk identification and assessment methodologies to obtain reasonable assurance of the completeness and accuracy of the risk register;
- Evaluate the effectiveness of mitigating strategies to address the material risks of the municipality;
- Report to the Municipal Manager and Audit Committee any material changes to the risk profile of the municipality;
- Review the fraud prevention policy and recommend for approval by the Municipal Manager and Council;
- Evaluate the effectiveness of the implementation of the fraud prevention policy;
- Review any material findings and recommendations by assurance providers on the system of risk management and monitor that appropriate action is instituted to address the identified weaknesses;
- Develop goals, objectives and key performance indicators for the Committee for approval by the Municipal Manager;
- Develop goals, objectives and key performance indicators to measure the effectiveness of the risk management activity;
- Set out the nature, role, responsibility and authority of the risk management function within the municipality for approval by the Municipal Manager, and oversee the performance of the risk management function;
- Provide proper and timely reports to the Municipal Manager and Audit Committee on the state of risk management, together with aspects requiring improvement accompanied by the Committee's recommendations to address such issues.

#### **6. Meetings**

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

#### **7. Administrative duties**

The Risk Officer, or such person as appointed by the Committee, shall be the secretary of the Committee. The secretary shall forward the notice of each meeting of the Committee to all members no later than seven working days prior to the date of the meeting. The notice shall confirm the venue, time, date and agenda and include the documents for discussion.

The minutes of the meetings shall be completed by the secretary and sent to all relevant officials for comment within XXX working days after the meeting.

The minutes shall be approved at the immediately following meeting, whereupon the approved minutes will be circulated to all attendees within XXX working days.

**8. Quorum**

50% plus one constitutes a quorum. A permanent member of the Committee may nominate a proxy on his / her behalf. This proviso shall lapse in the event that the permanent member fails to attend 50% or more of the Committee meetings held in that particular financial year in person.

**9. Performance evaluation**

The Committee shall evaluate its performance in terms of its charter at least annually.

**10. Review of the charter**

The Committee shall review the Charter annually and recommend to the Municipal Manager for approval any amendments that may be required.

## Annexure D

### **Suggested additional paragraphs for Audit Committee terms of reference (if acting as the oversight committee for risk management)**

#### **1 Enterprise Risk Management**

- (a) Gain a thorough understanding of the risk management policy, risk management strategy, risk management implementation plan, and fraud risk management policy of the municipality;
- (b) Review and critique the risk appetite and risk tolerance, and recommends this for approval by the Municipal Manager and Council;
- (c) Review the completeness of the risk assessment process implemented by management to ensure that all possible categories of risks, both internal and external to the municipality, have been identified during the risk assessment process. This includes an awareness of emerging risks pertaining to the municipality.
- (d) Review the risk profile and management action plans to address the risks;
- (e) Review the adequacy of adopted risk responses;
- (f) Monitor the progress made with the management action plan;
- (g) Review the progress made with regards to the implementation of the risk management strategy of the municipality;
- (h) Facilitate and monitor the coordination of all assurance activities implemented by the municipality;
- (i) Review and recommend any risk disclosures in the annual financial statements;
- (j) Provide regular feedback to the Municipal Manager and Council on the effectiveness of the risk management process implemented by the municipality;
- (k) Review the process implemented by management in respect of fraud prevention and ensure that all fraud related incidents have been followed up appropriately;
- (l) Review and ensure that the internal audit plans are aligned to the risk profile of the municipality;
- (m) Review the effectiveness of the assurance activities and recommend appropriate action to address any shortcomings.

## **Annexure E**

### **Template agenda for [MANCO] risk committee meeting**

1. Welcome
2. Apologies
3. Confirmation of the agenda
4. Minutes of the previous meeting
5. Presentations on specific risk profiles
  - a. Key risk a
  - b. Key risk b
6. New/emerging risks for consideration by the MANCO risk committee
7. Risks to be removed from the risk register
8. Insurance report
9. Occupational health and safety report
10. Incident and accident report
11. Compliance report
12. Ethics, fraud and whistle blowing incidents
13. Reports from assurance providers
  - a. Management
  - b. Internal Audit
  - c. External Audit
  - d. Other
14. Matters to be referred to the Audit Committee and/or Council
15. Closing
16. Date of next meeting




**Annexure F**





**Template risk register**

No.	Ref	Context/Category	Strategic goal	Risks	Cause	Consequence	Sub Risk	Likelihood	Impact	Inherent Risk	Risk owner	Existing Risk Mitigation / Current Controls	Control Effectiveness	Residual Risk	Desired Control Effectiveness	Desired Residual Risk	Risk Gap	Risk Mitigation Tasks	Task Owner	Due Date
<b>Example</b>	1.1	Operational Risk	4.3	Fire at key location	Electrical fault Arson Lightening strike	Loss of life/injury Loss/damage of key assets Loss of data		0.65	70.00	45.50	COO	Smoke detectors Electrical inspections Fire chief inspections Business continuity plan Insurance	0.65	29.575	0.4	18.2	11.375	Install automated fire suppression system and CCTV	Joe	25/12/2010
														0.00		0.00	0.00			
														0.00		0.00	0			

**Annexure G**

**Template Task Monitoring Report**

No.	Ref	Context	Risks	Cause	Consequence	Risk owner	Existing Risk Mitigation / Current Controls	Risk Mitigation Tasks	Task Owner	Due Date	Status (% completion)	Status Indicator
<b>Example</b>	1.1	Operational Risk	Fire at key location	Electrical fault Arson Lightening strike	Loss of life/injury Loss/damage of key assets Loss of data	COO	Smoke detectors Electrical inspections Fire chief inspections Business continuity plan Insurance	Instal automated fire supression system and CCTV	Joe	25/12/2010	0%	

Action status	
Indicator	Meaning
	Action Plan Overdue
	Action Plan due by the next report
	Action Plan on Schedule
	New Risks since last report