# GREATER GIYANI MUNICIPALITY

# RISK MANAGEMENT FRAMEWORK

## 2024/2025

## PREAMBLE

**PREFACE**

In line with the GGM's Risk Management policy, the Risk Management Framework must be reviewed annually when necessary. The 2023/24 Risk Management Strategy needed to be reviewed for an alignment with the proposed blueprint of the National Treasury 2017 for local government. The blueprint seeks to standardise the risk management processes across the Local.

In addition, a number of gaps were identified in the approved Risk Management Strategy 2023/24 and this revised Framework seeks to address the short comings.

CHAPTER 1

## 1. DEFINITIONS

The words used in Risk Management Framework bear the following meaning unless the context indicates otherwise:

| TERM | DEFINITION |
|---|---|
| Municipality | For the purpose of this policy, municipality shall mean Greater Giyani Municipality. |
| Accounting Officer | Means: The Municipal Manager as defined in terms of section 55 of the Municipal systems Act or any person delegated as such; |
| Audit Committee | Means: An independent advisory body constituted in terms of section 166 of the Municipal Finance Management Act 56/2003; |
| Chief Audit Executive | Means: A senior official within the Municipality responsible for Internal Audit Unit; |
| Manager Risk | Means: A senior official within the Municipality responsible for Risk Management unit; |
| Executive Authority | Means: Executive authority as defined in terms of section 11 of the Municipal Systems Amendment Act; |
| Internal Auditing | Means: An independent, objective assurance and consulting activity designed to add value and improve Municipality's operations. It helps the Municipality to accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. |
| King III | Means: The King Code of Corporate Governance for South Africa 2009. |

| TERM | DEFINITION |
|---|---|
| King IV | Means: The King Code of Corporate Governance for South Africa, 2016. |
| COSO Framework | Means: Committee of sponsoring Organizations of the Tredway Commission Internal Control-Integrated Framework |
| Other Official | Means: An official other than the Accounting Officer / Authority, Management, Manager Risk and his/her staff. |
| "Inherent Risk | Means: The exposure arising from risk factors in the absence of deliberate management intervention(s) to exercise control over such factors. |
| Residual Risk | Means: The remaining exposure after the mitigating effects of deliberate management intervention(s) to control such exposure (the remaining risk after Management has put in place measures to control the inherent risk). |
| Risk | Means: A threat (actual or potential) that causes uncertainty in the achievement the Council's Objectives |
| Risk Appetite | Means: The amount of residual risk that the Institution is willing to accept |
| Risk Champion | Means: A person who by virtue of his/her expertise or authority champions a particular aspect of the risk management process, but who is not the risk owner. |
| Risk Factor | Means: Any threat or event which creates, or has the potential to create risk. |
| Risk Management | Means: is a continuous, proactive and systematic process, effected by the Municipality's executive authority, accounting authority, management and other personnel, applied in strategic planning and across the Municipality, designed to identify potential events that may affect the Municipality, and manage risks to be within its risk tolerance, to provide reasonable assurance regarding the achievement of objectives. |
| Risk Management Committee" (RMC) | Means: A committee appointed by the Accounting Officer / Authority to review the Institution's system of risk management. |
| Risk Management Unit | Means: A business unit responsible for coordinating and supporting the overall Institutional risk management process, but which does not assume the responsibilities of Management for identifying, assessing and managing risk. |
| Risk Owner | Means: The person accountable for managing a particular risk. |

| TERM | DEFINITION |
|---|---|
| Risk Tolerance | Means: The amount of risk the Institution is capable of bearing (as opposed to the amount of risk it is willing to bear) |
| Action Owner | Means: The person responsible for the compilation and implementation of the action plan to mitigate a risk. |

## CHAPTER 2

### 2.1 PURPOSE

The purpose of this framework is to define the Local's risk management processes in order to ensure a consistent and a standardised risk management approach throughout the Greater Giyani Municipality. The framework seeks to guide the Council, Senior Management and all employees on risk management process. Lastly the framework seeks describe and outline roles and responsibilities for risk management within the Departments and Units, including communication and reporting requirements within the Local.

The framework takes into consideration and the guidelines on governance from the King IV on risk management. It is aligned to the COSO ERM Integrated Framework and ISO Risk Management Principles and Guidelines (ISO 31 000:2018).

The Framework has been developed in terms of the prescripts below

a) Sections 62(1) (c) (i) and 95(c) (i) of the MFMA, require the Accounting Officers to ensure that their municipalities and municipal entities have and maintain effective, efficient and transparent systems of risk management;

b) National Treasury Regulation 3(2) (1) requires the Accounting Officer to ensure that a risk assessment is conducted regularly to identify emerging risks of an institution. A risk management framework, which must include a fraud prevention plan, must be used to direct internal audit effort priority and to determine the skills required of managers and staff to improve controls and to manage these risks. The framework must be clearly communicated to all officials to ensure that the risk management is incorporated into the language and culture of the institution; and

c) National Treasury Public Sector Risk Management Framework.

## 2.2 KEY OBJECTIVES

The key objectives of this framework are:

2.2.1 To integrate Enterprise risk Management processes with organisational Strategy and Performance;

2.2.2 To effectively embed risk management processes and principles throughout the GGM Strategic objectives and goals;

2.2.3 To standardise the approach on risk management processes throughout the GGM;

2.2.4 To risk prioritise in order to ensure optimal risk management and positive results;

2.2.5 To provide management with proven risk management strategies that support decision making, while enhancing identification of key risk exposures and opportunities; and

2.2.6 To ensure continuous standardised communication and reporting to oversight committees.

## 2.3 TITLE AND APPLICATION

2.3.1 This framework shall be known as the Risk Management Framework of Greater Giyani Municipality.

2.3.2 This framework applies throughout the GGM in as far as the implementation of risk management is concerned. This policy applies to: -

2.3.2.1 All GGM Departments and business units;

2.3.2.2 All employees and officials of the GGM;

2.3.2.3 All key business projects;

2.3.2.4 The GGM's Council; Risk Management Committee; Audit Committee and all other governance structure; and

2.3.2.5 The Risk Management Unit.

## 2.4 COMMENCEMENT AND VALIDITY

2.4.1 This framework shall come into effect upon the acceptance hereof by the Council of the Greater Giyani Municipality by resolution.

2.4.2 The Greater Giyani Municipality shall ensure that employees, councillors and managers are informed about this policy and are trained to implement this framework effectively.

## 2.5 RELEVENT LEGISLATION, STANDARDS & CODES

This Framework was developed on the following legislative frameworks and leading best practice:

### 2.5.1 LEGISLATIVE:

2.5.1.1 Municipal Finance Management Act No. 56 of 2003;

2.5.1.2 Municipal Systems Act No. 32 of 2000, as amended;

2.5.1.3 Prevention and Combating of Corrupt Activities Act No. 12 of 2004

### 2.5.2 PUBLIC SECTOR AND LEADING PRINCIPLES STANDARDS & CODES

2.5.2.1 National Treasury Regulations April 2010;

2.5.2.2 COSO ERM Framework;

2.5.2.3 ISO 31000 2018;

2.5.2.4 King III and King IV Codes and Report on Good Governance

2.5.2.5 COBIT 5; and

2.5.2.6 Draft Local Government Risk Management Framework 2023/24

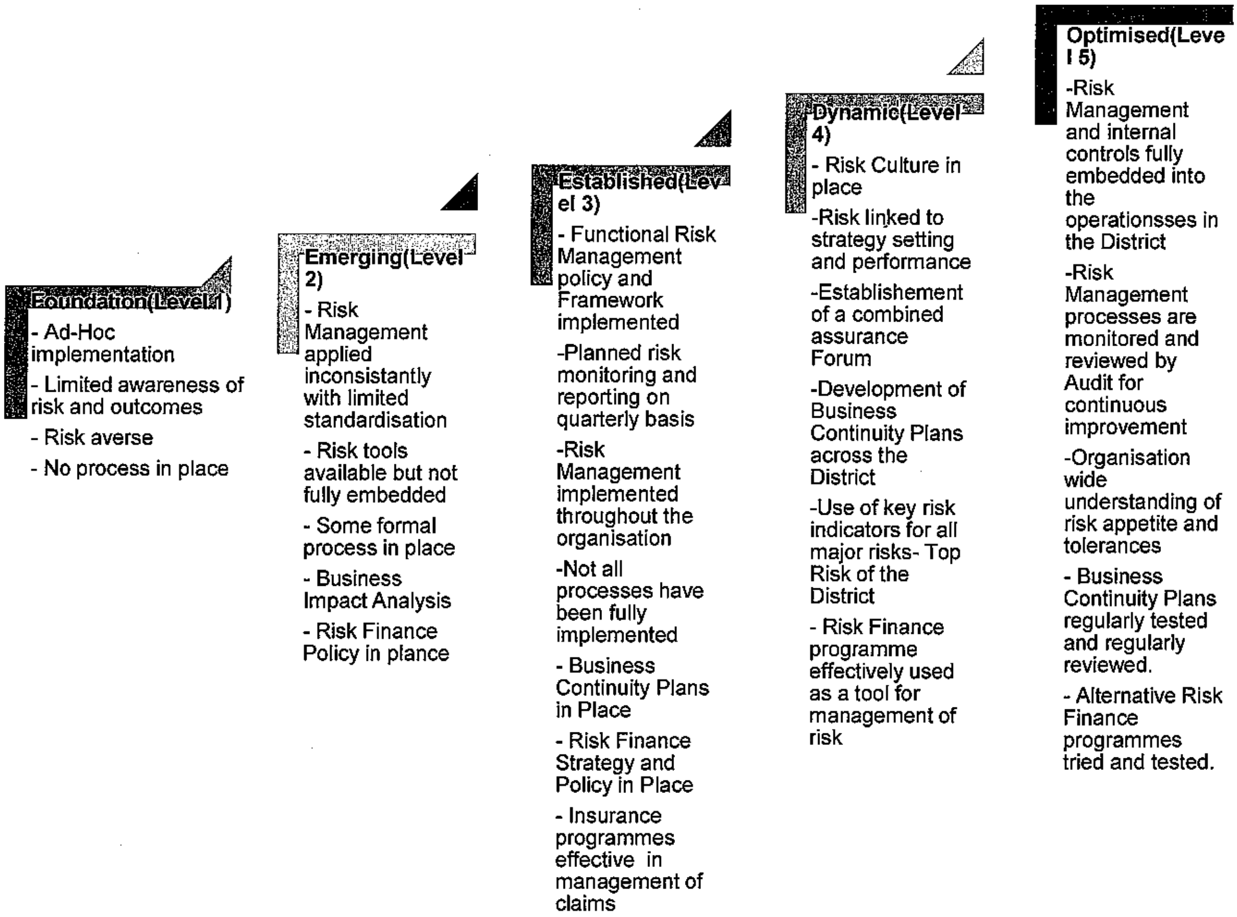
# CHAPTER 3

## 3.1 RISK MANAGEMENT MATURITY

Risk maturity is a benchmarking tool, which measures to what extent the Local, has implemented Enterprise Risk Management (ERM) in accordance with best practice. It helps establish the current risk maturity level so as to determine the desired future state that will support the Local's strategies and ultimately effect improvements on the ERM gaps identified. For the Local to achieve its desired risk maturity level, it requires, among others, adequate risk management capacity. Prior to implementing the ERM framework, the Local should assess if it has the risk management capacity that will enable it to implement the ERM framework and consequently achieve its desired level of risk maturity.

3.1.1 Risk Maturity Levels:

The Local's Risk Maturity level will be based on the Phases/ Stages as indicated in the diagram below. The Local must conduct an assessment of its maturity level every three years and ideally the level must be independently verified.



**Foundation(Level 1)**

- Ad-Hoc implementation
- Limited awareness of risk and outcomes
- Risk averse
- No process in place

**Emerging(Level 2)**

- Risk Management applied inconsistantly with limited standardisation
- Risk tools available but not fully embedded
- Some formal process in place
- Business Impact Analysis
- Risk Finance Policy in plance

**Established(Level 3)**

- Functional Risk Management policy and Framework implemented

-Planned risk monitoring and reporting on quarterly basis

-Risk Management implemented throughout the organisation

-Not all processes have been fully implemented

- Business Continuity Plans in Place
- Risk Finance Strategy and Policy in Place
- Insurance programmes effective in management of claims

**Dynamic(Level 4)**

- Risk Culture in place

-Risk linked to strategy setting and performance

-Establishement of a combined assurance Forum

-Development of Business Continuity Plans across the District

-Use of key risk indicators for all major risks- Top Risk of the District

- Risk Finance programme effectively used as a tool for management of risk

**Optimised(Level 5)**

-Risk Management and internal controls fully embedded into the operationsses in the District

-Risk Management processes are monitored and reviewed by Audit for continuous improvement

-Organisation wide understanding of risk appetite and tolerances

- Business Continuity Plans regularly tested and regularly reviewed.
- Alternative Risk Finance programmes tried and tested.

CHAPTER 4

## 4.1 CREATING AN ENABLING ENVIRONMENT

There are various enablers of effective risk management such as among others, the risk management framework within which the municipality should operate. The risk management implementation plan that guides the implementation of risk management framework, adequate capacity (financial, human, information and physical), clearly defined roles and responsibilities and establishment of appropriate risk management structures and processes.

The management and functioning of an organization is guided by, among others, its policies, procedures, methods and standards. The key enablers to effective risk management includes effective risk culture and internal control environment.

## 4.2 THE RISK CULTURE

The Institute of Risk Management of South Africa (IRMSA) defines the risk culture as the sum of the organisation's "shared values, beliefs, knowledge, attitudes and understanding about risk, shared by a group of people with a common intended purpose, in particular the leadership and employees of an organization.

According to the IRMSA an effective Risk Culture is viewed as the one that enables and rewards individuals and groups for taking risks in an informed manner. Council must consistently prioritise risk management and continually review the culture, people and processes.

## 4.3 COMPONENTS OF RISK MANAGEMENT

The process of managing risk is a structured approach for incorporating risk management into the daily, broader management process. Risk management is more than an exercise of risk avoidance. It is as much about identifying opportunities as avoiding or mitigating losses.

The control environment sets the tone of the Council and influences how strategies and objectives are structured; and the manner in which risks are identified, assessed and acted upon. It comprises many elements including the Municipality's ethical values, Integrity, discipline, competence, operating style, assigning of authority and responsibility.

Below are the set of interrelated components based on COSO Framework set of 17 principles for effective internal control:

| INTERNAL CONTROL COMPONENT | 17 PRINCIPLES | DESCRIPTION |
|---|---|---|
| Control Environment | Commitment to integrity and ethical values | The organization demonstrates a commitment to integrity and ethical values. |
| | Council responsibilities | The Council demonstrates independence from management and exercises oversight of the development and performance of internal control. |
| | Structures, reporting lines, authorities and responsibility | Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. |
| | Commitment to competent workforce | The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. |

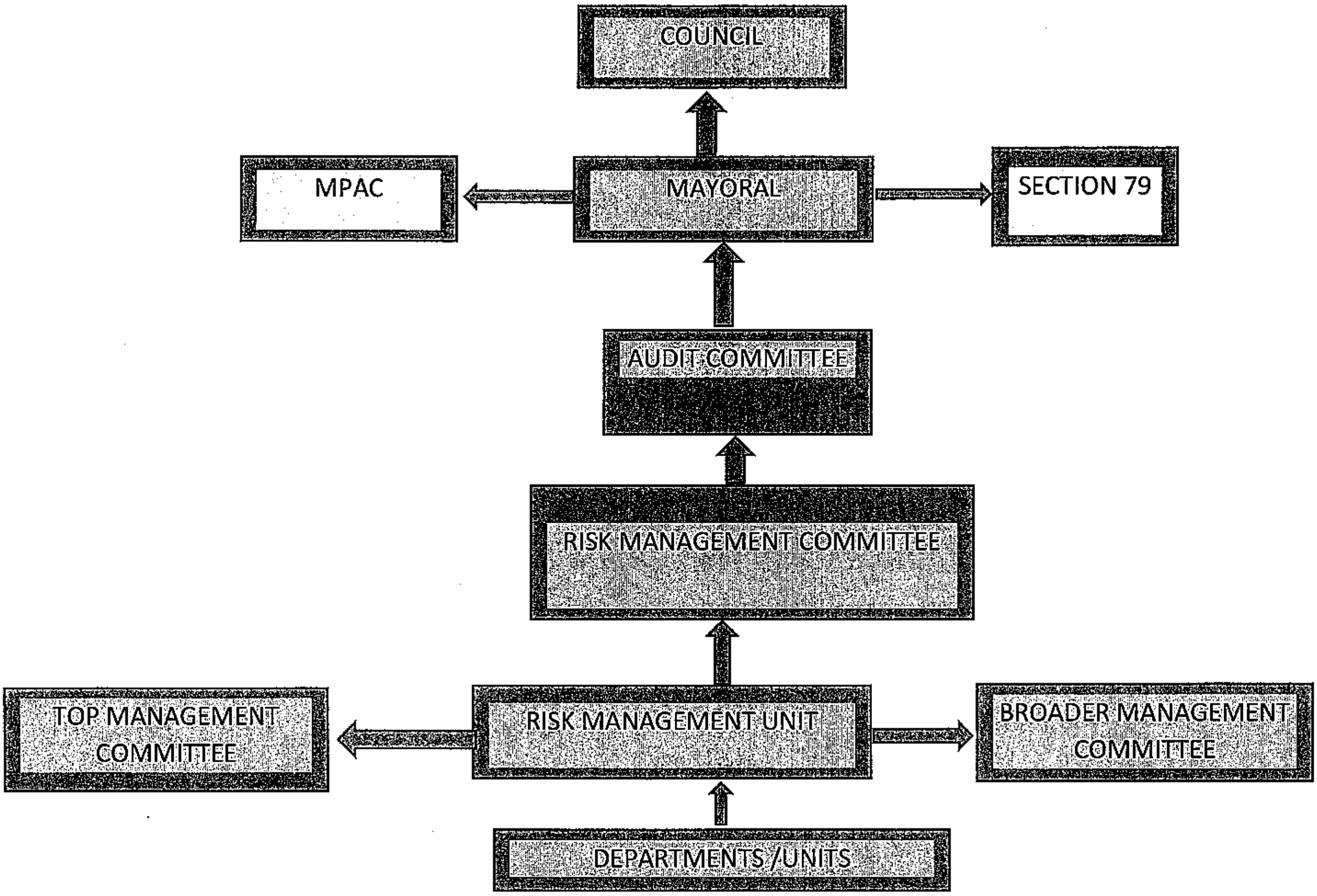
| INTERNAL CONTROL COMPONENT | 17 PRINCIPLES | DESCRIPTION |
|---|---|---|
| | Accountability | The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives. |
| Risk Assessment | Specification of objectives | The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. |
| | Identification and analyses of risks | The organization identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed. |
| | Evaluation of Fraud risks | The organization considers the potential for fraud in assessing risks to the achievement of objectives. |
| | Analyses of changes that could affect internal controls | The organization identifies and assesses changes that could significantly affect the system of internal control. |
| Control Activities | Development of control activities that mitigate or treats risks | The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. |
| | Select and develop technology controls | The organization selects and develops general control activities over technology to support the achievement of objectives. |
| | Deploy control activities though policies & procedures | The organization deploys control activities through policies that establish what is expected and procedures that put policies into action. |
| Information and Communication | Use relevant, quality information to support internal control function | The organization obtains or generates and uses relevant, quality information to support the functioning of internal control. |
| | Communicate internal control information internally | The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. |
| | Communicate internal control externally | The organization communicates with external parties regarding matters affecting the functioning of internal control. |
| Monitoring | Perform periodic evaluation of internal controls | The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. |
| | Communicate internal control deficiencies | The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior |

| INTERNAL CONTROL COMPONENT | 17 PRINCIPLES | DESCRIPTION |
|---|---|---|
| | | management and the board of directors, as appropriate. |

## 4.4.10. RISK MANAGEMENT GOVERNANCE

The Local's risk management governance structure, as set out in diagram 1 below, is designed to ensure that risk management process is effective throughout the Local:

**Diagram 1: Risk Management Structure and Reporting:**



## 4.5 ROLE AND RESPONSIBILITIES

| Role | Responsibility |
|---|---|
| Council | The Council should take an interest in risk management to the extent necessary to obtain comfort that properly established and functioning systems of risk management are in place to protect the Local against significant risk. |

| Role | Responsibility |
|---|---|
| | The high-level roles and responsibilities of the Council include:<br>▪ Ensure that the Local's strategies (IDP) are aligned to the government mandate.<br>▪ Obtain assurance from management that strategic choices were based on a rigorous assessment of risk;<br>▪ Obtain assurance that key risks inherent to the Local's strategies have been identified, assessed and that they are properly managed.<br>▪ Assist the Accounting Officer to deal with fiscal, intergovernmental, political and other risks out of the control of the Local.<br>▪ Insist on the achievement of objectives, effective performance management and value for money.<br>▪ Approve the risk management policy, framework, and implementation plan; and<br>▪ Approve the fraud prevention policy, strategy and implementation plan. |
| Accounting Officer | The Accounting Officer is the ultimate Risk Manager of the Local and is accountable for the Local's overall governance of risk.<br>High level responsibilities of the Accounting Officer include:<br>▪ Setting the 'tone' at the top on risk management principles, processes and governance structures.<br>▪ Delegating responsibilities for risk management to management and Risk Management Committee<br>▪ Holding management account for designing, implementation, monitoring and integrating risk management into their day-to-day activities.<br>▪ Holding internal structures accountable for performance in terms of their responsibilities for risk management<br>▪ Providing leadership and guide to enable management and internal structures responsible for various aspects of risk management to properly perform their duties<br>▪ Ensuring that the control environment supports the effective function of risk management.<br>▪ Approving the risk management framework<br>▪ Approving the Local's(Core) risk appetite and risk tolerance<br>▪ Providing assurance to oversight structures that key risks are properly identified, assessed and mitigated. |
| Risk Management Committee | The Risk Management Committee is appointed by the Accounting Officer / Authority to assist them to discharge their responsibilities for risk management.<br>In discharging its governance responsibilities relating to risk management, the committee should:<br>a) review and recommend for the Approval of the: |

| Role | Responsibility |
|---|---|
| | ▪ risk management policy;<br>▪ risk management framework;<br>▪ risk management implementation plan;<br>▪ risk appetite and tolerance framework;<br>▪ Institution's risk identification and assessment methodologies, after satisfying itself of their effectiveness in timeously and accurately identifying and assessing the Institution's risks.<br>b) evaluate the extent and effectiveness of integration of risk management within the Institution;<br>c) assess implementation of the risk management policy and framework (including plan);<br>d) evaluate the effectiveness of the mitigating strategies implemented to address the material risks of the Institution;<br>e) evaluate the effectiveness of the mitigating strategies implemented to address the material risks of the Institution;<br>f) review the material findings and recommendations by assurance providers on the system of risk management and monitor the implementation of such recommendations;<br>g) develop its own key performance indicators for approval by the Accounting Officer / Authority;<br>h) interact with the Audit Committee to share information relating to material risks of the Institution; and<br>i) Provide timely and useful reports to the Accounting Officer / Authority on the state of risk management, together with accompanying recommendations to address any deficiencies identified by the Committee. |
| Audit Committee | 1) The Audit Committee is an independent committee responsible for oversight<br>of the Institution's control, governance and risk management.<br>a) reviewing and recommending disclosures on matters of risk in the annual financial statements;<br>b) reviewing and recommending disclosures on matters of risk and risk management in the annual report;<br>c) providing regular feedback to the Accounting Officer / Authority on the adequacy and effectiveness of risk management in the Institution, including recommendations for improvement;<br>d) ensuring that the internal and external audit plans are aligned to the risk profile of the Institution;<br>e) satisfying itself that it has appropriately addressed the following areas:<br>- financial reporting risks, including the risk of fraud;<br>- internal financial controls; and<br>- IT risks as they relate to financial reporting.<br>f) The Audit Committee should evaluate the effectiveness of Internal Audit in its responsibilities for risk management. |
| Management | Ultimate responsibility for ERM starts at the top. The COSO ERM framework states that managers of the organization "support the entity's risk management philosophy, promote compliance with its risk appetite and |

| Role | Responsibility |
|---|---|
| | manage risks within their [respective] spheres of responsibility consistent with risk tolerances."<br><br>High level responsibilities of management as it relates to risk management include:<br>▪ Accountability to the Council/Board for designing, implementing and monitoring risk management, and integrating it into the day-to-day activities.<br>▪ Accountability for implementation of ERM Framework, policy and processes.<br>▪ Ensure that their risks are managed to a tolerable level and ensure that the risk register is in place and is continuously updated through regular risk assessments and updates to the control environment; and<br>▪ Providing reports and comment to oversight and assurance structures<br>▪ Acknowledge the "ownership" of risks within their business units or functional areas, and all responsibilities associated with managing such risks;<br>▪ Empowering officials to perform effectively in their risk management responsibilities through proper communication of responsibilities,<br>▪ Maintaining a co-operative relationship with the Risk Management Unit and Risk Champion<br>▪ Cascade risk management into its functional responsibilities; |
| Manager Risk | The Manager Risk has the overall responsibility to overseeing the risk management process within the Local. Manager Risk's responsibilities include the following:<br><br>▪ Provide and maintain risk management infrastructure<br>▪ Working with Executive Management to develop the Risk Management vision<br>▪ Developing, in consultation with management, Risk Management Framework incorporating inter alia:<br>- Risk Management Policy<br>- Risk Management implementation plan<br>- Risk Management Framework<br>- Risk appetite and tolerance framework<br>▪ Communicate the organization's risk management policy and framework and monitor the implementation<br>▪ Facilitate orientation for the Risk Management Committee<br>▪ Provide risk management training to stakeholders<br>▪ Continuously drive risk management to higher levels of maturity<br>▪ Assist management with risk identification, assessment and development of response strategies<br>▪ Monitoring the implementation of the responses |

| Role | Responsibility |
|---|---|
| | ▪ Reporting risk intelligence to Accounting Officer, management and Risk Management Committee<br>▪ Participating with Internal Audit, management and Auditor General to develop combined assurance plan for the organization<br>▪ Ensure that all the Local's assets are adequately insured |
| Risk Champion | A Risk Champion is person with skills, knowledge and leadership qualities and power of office required to champion a particular aspect of Risk Management within their respective department.<br><br>High level functions of a risk champion include:<br>▪ To champion the process of risk management within the team / organization, building commitment to and energy for the risk management process.<br>▪ Provide support as required to risk and action owners to help them routinely and accurately report progress for the risk response plans and to complete their actions in a timely manner.<br>▪ The Risk Champion should not assume the role of the Risk Owner but should assist the Risk Owner to resolve problems.<br>▪ To be familiar with risk tools required to support the team (e.g. risk register) and also the analysis tools that support specific functional risk analysis.<br>▪ Play an integral part in the risk assessment process by assisting in setting up workshops and participating in the risk assessment workshops.<br>▪ Forster a close relation with Group Risk Services to ensure alignment in risk practices within respective department. |
| Risk Management Units | A business unit responsible for coordinating and supporting the overall Institutional risk management process, but which does not assume the responsibilities of Management for identifying, assessing and managing risk.<br><br>A risk management unit/department is a separate and often independent unit within the organisation headed by the Risk Manager. The risk unit is primarily responsible for supporting management in discharging their risk management responsibilities as set out in this framework.<br><br>High level functions of a risk management unit include:<br>▪ Directly implement the Risk Framework and risk management policies and procedures.<br>▪ Identify and facilitate staff education on the Risk<br>▪ Management program, risk identification and reduction, expectations and strategies.<br>▪ Ensure identified strategies are put into place.<br>▪ Improving the risk maturity of the entity by implementing risk management techniques as guide by the Risk Framework<br>▪ Reviews all quality and risk related reports to identify trends, patterns, etc. |

| Role | Responsibility |
|---|---|
| | ▪ Monitors legislative activities that may affect risk management.<br>▪ Develop and monitor completion of annual RM implementation plan.<br>▪ Ensure alignment of entity's risk management practices to Group Risk practices and frameworks. |

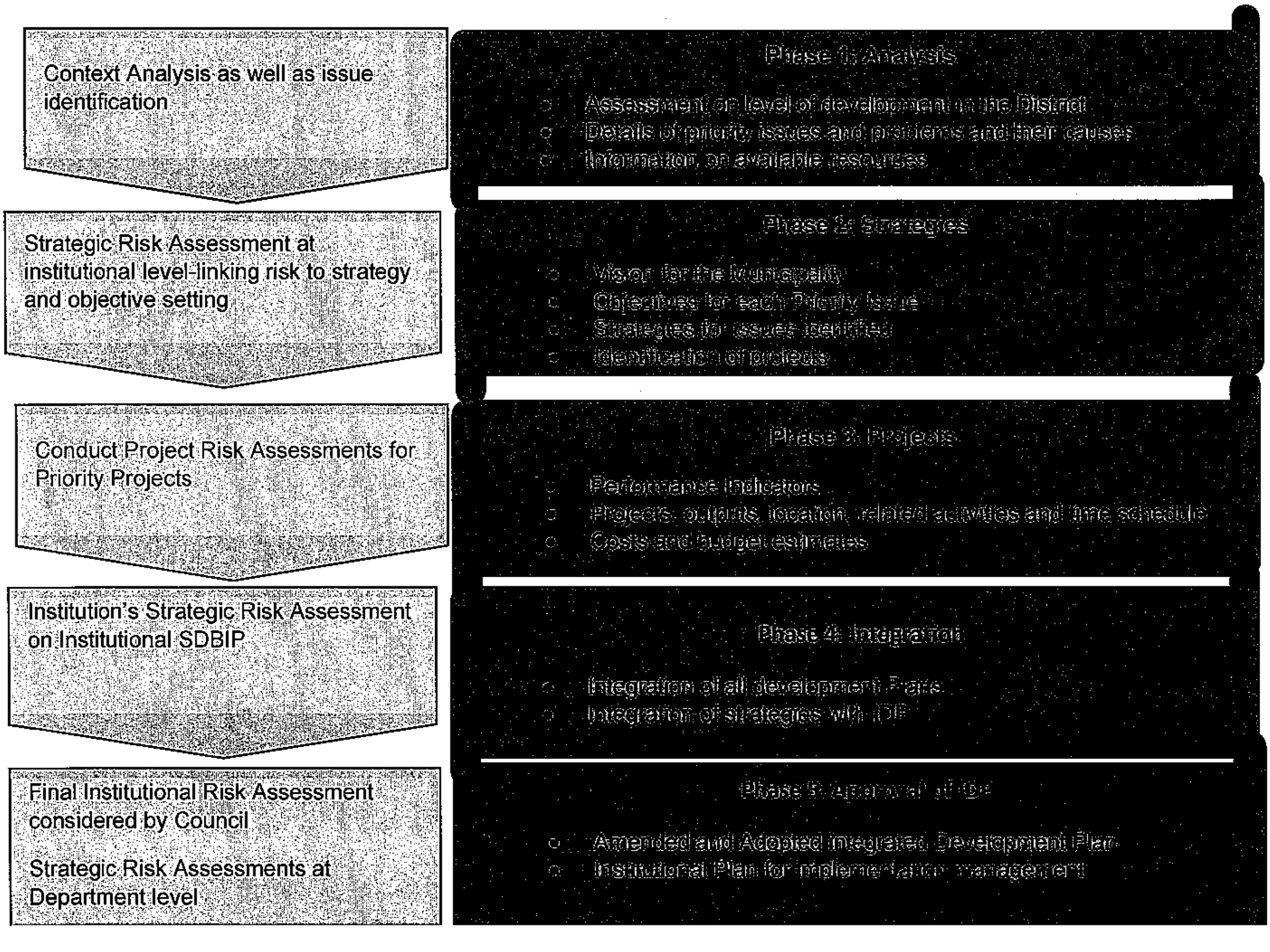
CHAPTER 5

## 1.1 INTERGRATION OF RISK MANAGEMENT

Integration of Risk Management, IDP and Planning Process

The IDP is a principal strategic and inclusive plan which guides and inform all planning, management and decision making at Local Government level. Risk is considered both at strategy setting process and is driving performance. Once the strategy is set, ERM provides an effective way for management to fulfil its role knowing that management is attuned to risks that can impact the strategy and is managing them well. A chosen strategy has to support the organizations mission and vision and ERM helps to identify, assess and manage risks to strategy. It also informs decision making that analyses risk and aligns resources with the mission and vision of the organization.

Enterprise Risk Management in the Local forms an integral part of Integrated Development Planning Process. The figure below illustrates these considerations.



Context Analysis as well as issue identification

Phase 1: Analysis

- Assessment on level of development in the District
- Details of priority issues and problems and their causes
- Information on available resources

Strategic Risk Assessment at institutional level-linking risk to strategy and objective setting

Phase 2: Strategies

- Vision for the Municipality
- Objectives for each Priority Issue
- Strategies for issues identified
- Identification of projects

Conduct Project Risk Assessments for Priority Projects

Phase 3: Projects

- Performance Indicators
- Projects: outputs, location, related activities and time schedule
- Costs and budget estimates

Institution's Strategic Risk Assessment on Institutional SDBIP

Phase 4: Integration

- Integration of all development Plans
- Integration of strategies with IDP

Final Institutional Risk Assessment considered by Council

Strategic Risk Assessments at Department level

Phase 5: Approval of IDP

- Amended and Adopted Integrated Development Plan
- Institutional Plan for implementation management

In order to apply holistic risk monitoring approach effectively, risk monitoring process should be linked to Performance Management. This is to ensure sufficient integration between risk management and performance measures through tracking the risks using KPIs/ objectives.

## 1.2 DEVELOPING KEY RISK INDICATORS

Key Risk indicators (KRIs) refers to metrics or indicators to be used to effectively identify potential future risk conditions so that management are able to be more proactive on potential impacts on Local's overall risk profile, enabling them to be more in a better position to manage events that may arise in the future, on a more timely and strategic basis.

The development of effective KRIs starts by proper understanding and analysis of Local's objectives. The constant measure and monitoring of KRIs provides value to the Local in a variety of ways and bring the following benefits:

- Risk and Opportunity Identification: KRIs are designed to alert management to trends that may adversely affect the achievement of Local objectives, or may indicate the presence of new opportunities;
- Risk Treatment: KRIs initiate action to mitigate future risks by serving as triggering mechanisms to improve controls and implement action plans;
- Risk Reporting: Relevant risk intelligence summary reports are promptly communicated to appropriate senior or executive managers and MOE boards and oversight committees.

## 1.3 COMBINED ASSURANCE

Combined assurance is based on the identified Top/Key Strategic Risks for the Local and how assurance is achieved and reported to Assurance Committee.

This risks profile is used to establish what risks are assured and by whom. The different lines of defence are mapped to the identified risks in terms of work actually performed and the assurance expected.

The combined assurance model identifies, and assigns accountability and responsibilities to three defines levels, with the first level being Management; second level being Internal Assurance Providers and the third level being External Assurance providers.

By its nature, Combined Assurance requires collaboration and synergy. The Internal Audit Unit will not be able to provide absolute assurance on the entire universe every year; therefore all Three (3) lines of defines (assurance providers) play a critical role in providing adequate assurance to the Governance Committees and management.

The table below outlines the levels of assurance providers:

| 1st Line | 2nd Line | 3rd Line | 4th Line |
|---|---|---|---|
| Management oversight | Management of risk and Compliance | Internal audit | Independent external assurance |
| Risks owners and Action owners:<br>• Heads of Department /Units and<br>• Risk Champions | Includes functions such as<br>• HR,<br>• SCM,<br>• Compliance,<br>• Legal,<br>• Risk Management,<br>• Health & Safety. | Internal Audit oversight | Includes:<br>▪ Auditor General;<br>▪ Audit Committee |
| Actual management of risks (strategic and operational) and performance. Systems for self-assessments must be put in place and implemented to address adequacy of risk management. | Provides management with support in executing their duties and their management of risks. | Provides internal risk-based audits and provides independent assurance over controls, risk management and governance. | Conducts statutory and regulatory audits.<br>Independent oversight. |

## 1.4 RISK APPETITE AND RISK TOLERANCE

An integral part of ERM is the development of key risk metrics, exposure limits, and governance and oversight processes to ensure enterprise-wide risks are within acceptable and manageable levels. A best-practice approach to addressing these requirements is to implement a clearly defined risk appetite and tolerance model. Risk Appetite is defined as the level of risk the Municipality is willing to accept in the pursuit of its strategic objectives and risk tolerance is the amount of risk the Municipality is prepared to bear above the risk appetite in pursuit of its strategic and objectives. Risk tolerance relates to the level of risk that an organization can accept per individual risk, whereas risk appetite is the total risk that the organization can bear in a given risk profile, usually expressed in aggregate. The Greater Giyani Municipality has in place a Risk Appetite and Tolerance Framework to guide the development of Risk Appetite and Tolerance levels.

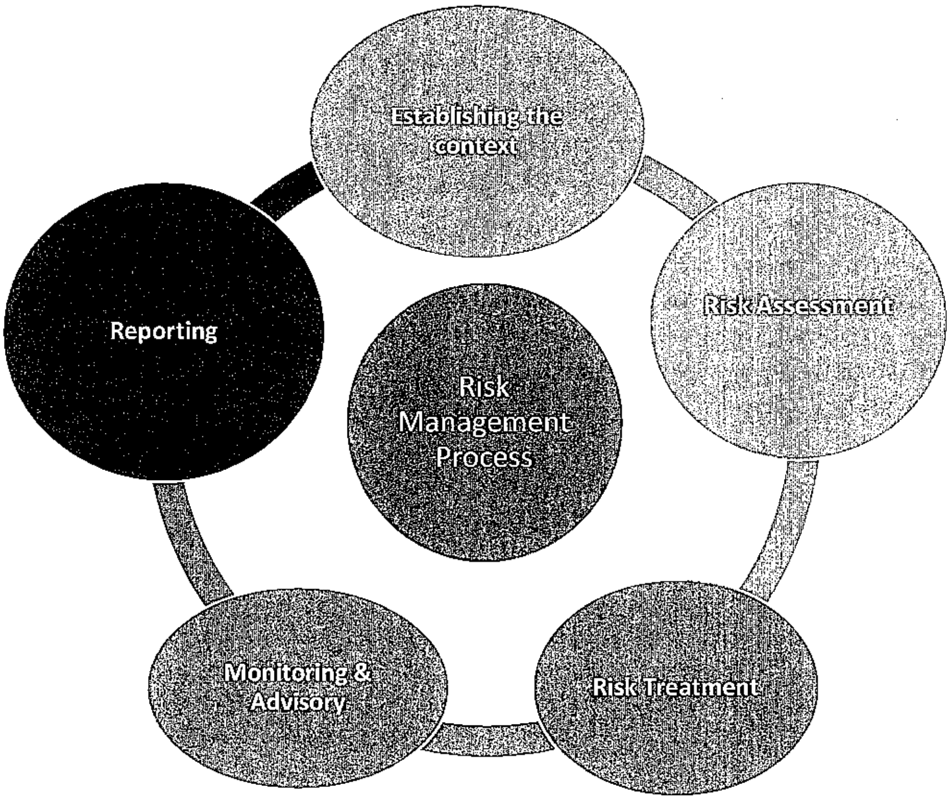
Risk appetite is a cornerstone of a successful risk management, and therefore the effective correlation of the two into performance management systems is highly crucial. Similarly, measures should be included in the scorecards for Executives and Senior Management.

An effective risk appetite needs to be integrated into Local-wide decision-making processes. Integration into governance and reporting, that includes development of governing frameworks, policies and procedures, escalation and delegation authority, and appropriate mitigating strategies in the events that tolerance limits are exceeded.

CHAPTER 6

## 6.1 RISK MANAGEMENT PROCESS

**The diagram below indicates the Local's risk management process;**



### 6.1.1 COMMUNICATION AND CONSULTATION

The Local communication is structured to identify who (internally and externally) should receive what information, to generate the information required and to communicate it on time and in an effective manner. The communication and consultation taking place should be truthful, relevant, accurate and understandable, taking into account confidentiality and personal integrity.

An effective external and internal risk communication and consultation strategy will ensure that all the role-players who are responsible for the risk management process, as well as all the other stakeholders, understand the reasons for and the actions required by risk-related decisions.:

### 6.1.2ESTABLISHING THE CONTEXT

The Local articulate its objectives, defines the external and internal parameters to be taken into account when managing risk and sets the scope and risk criteria.

The following documentation is utilised as primary source when identifying risks in the Local:

- Integrated Development Plan (IDP):
- Service Delivery Business Implementation Plans (SDBIPs);
- Performance Scorecards;
- Internal and external factors;
- External and internal audit reports;
- Financial reports;
- Historic data and past experiences;
- Interrogation of trends in Key Performance/Risk Indicators (KPIs/KRIs);
- Local's Risk Universe; and
- Benchmarking against appropriate peer organisations.
- IRMSA risk report
- Risk Appetite and Tolerance framework

### 6.1.3 RISK ASSESSMENT

At this stage Greater Giyani Municipality identify what could cause an the Local to deviate from its objectives, to determine how likely it is to happen, as well as what the consequences could be if it does happen. Subsequent to this, the organisation needs to determine which risks need to be addressed first, which risks are less urgent and which risks do not warrant intervention.

GGM's Risk assessment is a structured process that:

- Identifies how the Local's objectives could be affected by risks.
- Analyses the risk in terms of its consequences and probabilities of occurrence, along with what type of risk it is.
- Describes the priority that should be assigned to each risk.

The Local has adopted both 'top-down' and 'bottom-up' risk assessment approach.
Risk assessments are conducted on:

- Local wide level Organisational;
- Departmental and Entity Strategic levels;
- Department and Operational levels;
- Projects and Contracts;
- Information and Communication Technology (ICT); and
- Ethics ,Fraud and Corruption.
- Physical Risk Assessment
- Post Loss Assessment

The responsibility to ensure that periodic risk assessments are conducted for each business unit rests with the executive and senior management.

## I. STRATEGIC RISK IDENTIFICATION

Strategic risk identification precedes the finalisation of strategic goals and objectives to ensure that potential risks are factored into the decision making. Risks inherent to set strategic goals and objectives are documented, assessed and managed through the adopted risk management principles.

The strategic risk assessments are conducted annually and reviewed quarterly parallel to Council's planning cycles.

## II. OPERATIONAL RISK IDENTIFICATION

Operational risk identification seeks to uncover all the uncertainties introduced by day-to-day implementation/operating processes and activities. Operational risk identification is an embedded process into management's daily operations to identify new and emerging risks to consider process reviews and formal operational risk assessment processes.

Operational risk assessments are conducted annually and reviewed quarterly parallel to Council's planning cycles.

## III. INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) RISK IDENTIFICATION

ICT risk management is the application of risk management methods to Information technology in order to manage ICT risks, that is, the business risks associated with the use, ownership, operation, involvement, influence and adoption of IT strategies Local-wide. IT benefit/value enablement risks are associated with opportunities to use technology to improve efficiency or effectiveness of business processes, or as an enabler for new business initiatives.

## IV. PROJECTS AND CONTRACT RISK IDENTIFICATION

Projects and contracts are the key drivers and enablers to the Local's achievement of its service delivery agenda. The objective of projects and contracts risk identification is to identify risks inherent to a particular or significant Local projects and contracts. Projects and contract risk assessments are conducted and reviewed periodically taking into consideration the life cycles of projects.

Risk management is considered to be a part of the overall project management, an exercise in which risks are identified, mitigation actions applied, and mitigation plans are developed. More often, projects fail due to a lack of risk management strategies at project level. The primary purpose of a project risk management is to maximise return on investment (ROI).

Local's approach to project risk management, addresses particularly those risks associated with both type of the project and the nature of the professional services required or being provided.

In order to ensure that the project risk assessment becomes a meaningful exercise, the Senior Managers should ensure that an annual identification of Local's top contracts (monetary value) for assessment and monitoring.

## V. ETHICS, FRAUD RISK IDENTIFICATION

Ethics, Fraud and Corruption is an intentional act or omission designed to deceive others, resulting in a victim suffering a loss/and or the perpetrator achieving a gain. Fraud risk governance is an integral component of corporate governance and an internal control environment.

Ethics, fraud and corruption risk assessment is a dynamic and iterative process for identifying and assessing ethics, fraud and corruption risk relevant to the organisation. Ethics, Fraud and Corruption Risk Assessment addresses the following risks:

- Fraudulent Financial Reporting
- Fraudulent Non-Financial Reporting
- Asset Misappropriation
- Illegal acts including corruption
- Conflict of interest
- Nepotism and favouritism

## VI. OCCUPATIONAL HEALTH AND SAFETY(OHS) RISK ASSESSMENT

An OHS risk assessment is a process to identify potential hazards and analyses the consequences should the hazards occur. Significant areas for repairs and maintenance should be highlighted to ensure that appropriate measures are undertaken.

The purpose of OHS risk assessment is:

- to ensure adequate asset maintenance,
- to protect Local's properties against hazards, loss/ theft,
- to avoid financial losses (including public liability)
- to ensure insurability of the assets/property
- to avoid danger to and/ or loss of life,
- to avoid litigations and
- to ensure compliance with Occupational Health and Safety Act (OHASA)

## VII. OHS Risk Control is divided into three parts:

- Avoid the risk;
- Reduce the risk and
- Prevent the risk from occurring

## VIII. Five Steps to OHS Risk Assessment

- Identify the hazard;
- Decide who might be harmed and how;
- Evaluate the risk and decide on precaution;
- Record the findings in the Physical Risk Assessment Report;
- Review the assessment and update if necessary

## IX. POST LOSS ASSESSMENTS

Post loss assessment are carried out across a range of events including:

- Property loss due to fire and or machinery breakdown,
- Property loss due to hazards
- Property loss due to theft
- Property loss due to pollution,
- Business interruption following property damage,
- Business interruption following casualty events
- Workplace and third-party health and safety.

## X. Post Loss Analysis Report

The analysis report consists of the following information:

- Details of loss including history;
- Cause of the loss;
- Estimated financial impact of the loss;
- Appraisal of pre-existing protection systems and an assessment of their effectiveness in reducing the loss and
- Cost effective measures that should be considered to avoid or mitigate potential future losses.

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

### 6.1.4 Risk identification

The aim of this step is to generate a comprehensive list of risk based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives.

The risk associated with not pursuing an opportunity are also identified. Identification include risk whether or not their sources is under the control of the Local, even though the risk source or cause may not be evident.

Risk identification also draws as much as possible from unbiased independent sources, including the perspectives of important stakeholders.

The identification include risks whether or not their source is under the control of the Local, even though the risk source or cause may not be evident.

The following techniques may be used for identification of risks:

- Risk workshops;
- Interviews;
- Questionnaires ; and
- Observations

### 6.1.5 Risk analysis

The Risk analysis involve developing of the risk. Risk analysis provide an input to risk evaluation and to decision on whether risk need to be treated, and on the most appropriate risk treatment strategies and methods.

The risk analysis involve consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur.

#### 6.1.5.1 RISK CATEGORIES

As the risk environment is so varied and complex it is useful to group potential events into risk categories. By aggregating risk events horizontally across the Local, and vertically within departments, MOEs, business units, and priority programmes, management develops an understanding of interrelationships between risk events, and gaining enhanced information as a basis for risk assessment.

All risks identified are allocated to an applicable risk category. External and internal risk categories are outlined on tables below;

Strategic Risk Categories:

| No | Risk Category | Explanation of Risk Category |
|---|---|---|
| 1. | **External Environment** | Service delivery related risks |
| 2. | **Economic Risk** | Inflation, investments, economic growth, economic infrastructure, economic down grades and upgrades. |
| 3. | **Financial** | Liquidity, cash flow, solvency, going concern, tariff risk, credit risk, financial instruments, cost of risk finance, cost of capital, collaterals. |
| 4. | **Technology Risk** | ICT Governance, changes in technology environment, cyber threats, hacking, phishing. |
| 5. | **Regulatory requirement risk** | Significant changes in legislation, Compliance, Misinterpretation of legislation. |
| 6 | **Political** | Political change/ changed political leadership. |
| 7. | **Socio Economic** | Crime, Poverty, Inequality, unemployment, illegal immigration, population growth, diseases |
| 8. | **Environmental** | Risk as a result of climate change, air pollution and depletion of natural resources. |
| 9. | **Stakeholder Management risk** | Risks impacting on stakeholder relations and trust. |
| 10. | **Human Capital** | Affecting Staff / skills |

Operational Risk Categories:

| No | Risk Category | Explanation of Risk Category |
|---|---|---|
| 1. | **People** | Human Errors, unethical practices, loss of key personnel , breaches of employment law, unauthorised activities, inadequate training etc. |
| 2. | **Processes** | Transactions |
| 3. | **External Environment** | Utility failure, crime, regulatory risks, outsourcing risks. |
| 4 | **Systems** | Unauthorised use of information technology, technology changes, business interruption, technological/ network |

| No | Risk Category | Explanation of Risk Category |
|---|---|---|
|  |  | failure, power failure, backup failure, obsolete software and systems etc. |

**Ethics, Fraud and Corruption risk categories:**

| No | Risk Category | Explanation of Risk Category |
|---|---|---|
| **1.** | **Human Resources** | Recruitment, Payroll Fraud, Misrepresentation |
| **2.** | **Asset Misappropriation** | Cash and non-cash |
| **3.** | **Fraudulent Statements** | Financial and non-financial |
| **4** | **Corruption** | Conflict of interest, Bribery and extortion |

**Project and Contract Risk Categories:**

In the case of contracts, the key risks can be categorised into main broader areas as follows;

| Risk Category | Details |
|---|---|
| Service failure | This is the most common risk is that the supplier might not deliver the service to the standard or timeliness specified in the contract. Service failure can range from a relatively minor shortfall against required service levels, to a complete failure. |
| Litigation | Both parties might be in breach of contract |
| Reputational damage | In some manner, the supplier may cause harm to the Local's reputation, for example, the supplier may act illegally or in a manner that conflicts with government policies. Poor performance by the supplier may also cause reputational damage to the Local. |
| Additional cost | This category of risk covers cases where the contract costs increase more than expected or budgeted, and those costs do not represent value for money. |

### 6.1.6Risk Evaluation

The purpose of risk evaluation is to assist in making decisions, based on the outcome of risk analysis, about which risks need treatment and the priority for treatment implementation.

Decision should take account of the wider context of the risk and include consideration of the tolerance of the risks borne by parties other than the Local that benefits from the risk.The decision is made in accordance with legal, regulatory and other requirements.

**RISK EVALUATION AND MEASUREMENT**

## 1. RISK RATING AND RANKING

In any assessment exercise, it is essential that risks are not only identified, but also rated and ranked (prioritized). This is done by rating your risks based on the likelihood (probability) of occurrence and the impact thereof, should that risk materialize. For the purpose of this workshop we will be considering inherent risks, i.e. the risk to the organization in the absence of any actions management might have taken to alter either the specific risks likelihood or impact.

For every risk it is important that you consider the nature and the scope of the risk and then rate the risk accordingly. Risks will be individually ranked by each participant.

### 4.1. Rating on Impact

When rating a risk on the impact of the risk on the business, should it occur, you need to consider what the extent of the impact of that risk will be on the area of the business, which it affects. Some risks may have a major impact one objective, yet a fairly low impact on the organization as a whole.

> **"Impact can be defined as the material loss to the organization, should that risk materialize"**

**Impact will be rated on a scale of 1 to 5 as follows**

| **Example: Impact on service delivery** | | |
|---|---|---|
| **Score** | **Impact** | **Consequence** |
| **5** | Critical | Negative outcomes or missed opportunities that are of critical importance to the achievements of the objectives |
| **4** | Major | Negative outcome or missed opportunities that are likely to have a relatively substantial impact on the ability to meet objectives. |
| **3** | Moderate | Negative outcome or missed opportunities that are likely to have a relatively moderate impact on the ability to meet objectives. |
| **2** | Minor | Negative outcomes or missed opportunities that are likely to have a relatively low impact on the ability to meet objectives. |
| **1** | Insignificant | Negative outcomes or missed opportunities that are likely to have a negligible impact on the ability to meet objectives |

### 4.2. Rating on Likelihood (probability)

When voting on the likelihood of a risk materiality, we will be considering the possibility that the given event or risk or reduce the probability of the risk materializing.

> **"Likelihood can be defined as the probability of an adverse event, which could cause materialisation of the risk, may occur."**

**Likelihood will be rated on a scale of 1 to 5:**

| **Example: Certainty of occurrence** | | | |
|---|---|---|---|
| **Score** | **Likelihood** | **Description** | **Probability** |
| **5** | Common | The threat may occur within the period of assessment | The probability of exposure has occurred repeatedly |
| **4** | Likely | The threat is likely to occur in a short term (1 to 3 years) | High probability this exposure will occur |
| **3** | Moderate | The threat could occur in long term (3 to 5 years) | There's a strong probability this exposure will occur in some instances |
| **2** | Unlikely | Very few recorded or known incidents occurred within other organisations within the sector | Probability in rare or exceptional circumstances |
| **1** | Rare | Threat may occur in exceptional circumstances | Probability is remote |

Applying the parameters to the risk matrix to indicate what areas of the risk matrix would be regarded as high, medium or low risk (see the example below);

**Risk Index = Impact X Likelihood**

| | | | | | | |
|---|---|---|---|---|---|---|
| **I** | **5** | 5 | **10** | 15 | | |
| **M** | **4** | **4** | [illegible] | **12** | 16 | |
| **P** | **3** | **3** | [illegible] | [illegible] | **12** | 15 |
| **A** | **2** | **2** | **4** | | | **10** |
| **C** | **1** | **1** | **2** | **3** | **4** | 5 |
| **T** | | **1** | **2** | **3** | **4** | **5** |
| **Likelihood** | | | | | | |

→

| | |
|---|---|
| | |
| 15 - 19 | High risk |
| 10 - 14 | Medium risk |
| 5 - 9 | Low risk |
| 1 - 4 | Minimum risk |

**Determine risk acceptability and what action will be proposed to reduce the risk below**

| Risk Index | Risk Magnitude | Risk Acceptability | Proposed mitigating steps |
|---|---|---|---|
| | | | |
| 15 - 19 | High risk | Unacceptable risk | Implementation of improvement opportunities and validation of current controls |
| 10 - 14 | Medium risk | Unacceptable risk | Evaluation and improvement of current controls |
| 5 - 9 | Low risk | Accept Risk | Validation and optimization of controls |
| 1 – 4 | Minimum risk | Accept Risk | No risk reduction – control, monitor, inform management |

**Scale for evaluation of risk impact**

| Severity Ranking | Financial | Service Delivery/External Environment | Reputation/Stakeholder | Human Capital | Systems/Technology | Environment |
|---|---|---|---|---|---|---|
| Insignificant<br>1 | • Financial Loss of less than0.5% of budget<br>• Insurance Claims more than R2m<br>• Loss of less than 10% revenue | Negligible impact on achievement of quarterly service delivery targets and objectives or no performance reduction | •Occasional complaints with no or insignificant impact<br>•Reputation intact<br>• Minimal impact on stakeholder support | Minor or very low staff attrition rate (<4%) | Key systems are not operative for half a day | Short term transient impact on environment or community negligible action required |
| Minor<br>2 | • Financial Loss of more than 2% of budget<br>• Insurance Claims more than R4m<br>• Loss of more than 20% revenue | Negative impact on achievement of quarterly service delivery targets and objectives or minor performance reduction | •Intra-sector knowledge of incident, but no media attention.<br>• Marginal decrease in stakeholder support | Staff attrition (>4% but <10%) on an annual basis) | Key systems not in operative for less than 24 hours | Medium term, immaterial effect on environment. |
| Moderate<br>3 | • Financial Loss of more than 5% of budget<br>• Insurance Claims more than R6m<br>• Loss of more than 30% revenue | • Negative impact on achievement of targets in more than 1 year<br>Service delivery disruptions in more than 1 year | •credibility and/or investors lost in more within 2 years<br>•Adverse national media coverage (national TV headlines) and loss of service in more than 1 year. | Key skilled staff lost (>10%but <25%) in 1 year | Key systems not in operative for 1 day | Measurable environmental harm caused medium tern recovery<br>Community complaints voiced privately |
| Major<br>4 | • Financial Loss of more than 10% of budget<br>• Insurance Claims more than R8m<br>• Loss of more than 40% revenue | • Negative impact on achievement of targets within 1 year.<br>• Service delivery disruptions in 1 | • credibility and/or investors lost in more than 1 Year<br>• Adverse national media coverage and loss of service >1 | Certain key executives and/or key employees and skills (>25% but <50%) are lost in 1 year | Key systems not in operative in 2 days | Harm to environment and community health and living standards in |

| Severity Ranking | Financial | Service Delivery/External Environment | Reputation/Stakeholder | Human Capital | Systems/Technology | Environment |
|---|---|---|---|---|---|---|
| | | year. Qualified annual external audit reports every year. | year. Medium term public impact with minor political implications. | | | more than 1 year |
| Critical<br>5 | • Financial Loss of more than 15% of budget<br>• Insurance Claims more than R10m<br>• Loss of more than 50% revenue<br>• Loss of creditworthiness in 1 year | • Negative impact on achievement targets in > 1 year<br>• service delivery disruptions in >1 year<br>• Non delivery of key objectives<br>• Major impact on the operational viability that may lead to work or task cancellation<br>• Qualified annual external audit reports every year | • Credibility and/or investors lost < 1 Year.<br>• Stakeholder relations lost > 1 Year.<br>• Adverse national media coverage and loss of service >1 month.<br>• Employees may have suffered fatalities. Event may have resulted in staff loss causing catastrophic consequences | Loss of key personnel and skills (50% or more) in 1 year | Key Systems in operative for 3 -5 days | Harm to environment and community health and living standards in > 1 year |

## 6.1.7 RISK TREATMENT & RESPONSE

The updated COSO Internal Control Framework, 2016 "An organisation selects control activities that contributes to the mitigation of risk to the achievement of objectives to the acceptable level. The organisation deploys control activities through policies that establish what is expected and procedures that put policies into action.

ISO 31000:2009 Risk management Principles and guidelines defines control as a "measure that is modifying risk" and includes "any process, policy, device, practice, or other actions". All Local employees have a role for maintaining effective systems of internal control, consistent with risk management strategies.

Risk treatment involves selecting one or more options for modifying risks, and implementing those options. Once implemented, treatments provide or modify the controls.

Risk treatment involve a cyclical process of:

- Assessing a risk treatment
- Deciding whether residual risk level is tolerable;
- If not tolerable, generating a new risk treatment; and
- Assessing the effectiveness of that treatment.

The Local has adopted the following risk treatment options:

Risk responses are strategies developed to mitigate and reduce risks from materialising. The Local endeavours to optimally control and manage risk exposures to an acceptable level, and to ensure that exposures are not realised. The Local has adopted the following risk response strategies based on The IRMSA Guideline to Risk Management:

| No | Response Strategy | Explanation of Strategy |
|---|---|---|
| **1.** | Accepting or tolerating the risk | The organisation may decide to accept the level of risk inherent to an event and continue to pursue its objectives. This may occur if or when the management team believes that the costs of responding to the risk do not create or protect sufficient value to justify additional effort. In this case, it may be better to simply accept the positive or negative consequences, integrate the risk into existing processes and incorporate the learning into future decisions. |
| **2.** | Avoiding the risk | The organisation may decide to completely avoid this specific risk by deciding not to pursue or continue the activity that gives rise to the risk exposure. This means that the organisation will not suffer the consequences but will also not have the opportunity to benefit from the activity. |
| **3.** | Removing the source of risk | It may be possible under particular circumstances to remove the source of risk from the activity. This is particularly the case if it is a technology or asset that can be disposed of, substituted or replaced. This option can be applied in other ways as well, for example by changing (an aspect of ) the operating model of the organisation. |
| **4.** | Changing the likelihood | It may be possible to influence the likelihood of an event. This option usually adjusts either the operating processes or human behaviour that give rise to a particular risk. An example would be introducing mandatory rest breaks for long-distance drivers (thus reducing the likelihood of accidents), or increasing the acceptance criteria for issuing short-term debt (thereby improving the quality of debtor, and hence decreasing the likelihood of default). These are also known as preventative controls. |

| No | Response Strategy | Explanation of Strategy |
|---|---|---|
| 5 | Changing the consequence | A variety of techniques can affect the severity of a particular risk. These involve a detailed understanding of the consequences, and who experiences them. This can range from the provision of fire-fighting equipment as a measure of last resort to maintaining an effective emergency response plan for certain catastrophic operational events. These are often known as corrective controls. |
| 6 | Transferring the risk | A final option is to transfer the risk (at a price) to another party or parties; this usually focuses on the financial consequences of a risk (e.g. loss of income, unexpected expenditure). This may include contractual agreements, outsourcing, risk financing and insurance. Risk transfer is a risk management technique whereby risk of loss is transferred to another party through a contract (e.g., a hold harmless clause) or to a professional risk bearer (i.e., an insurance company) normally at a fee or premium.<br>Risks that are transferred normally refer to activities with low probability of occurring, but with a large financial impact. The best response is to transfer a portion or all of the risk to a third party by purchasing insurance, hedging, outsourcing, or entering into partnerships. |
| 7 | Exploit the opportunity | For positive risks, the organisation may wish to allocate additional resources to exploit and benefit from the uncertainty. This is often the case when external trends or factors move in the organisations favour (such as movements in the exchange rate, relaxation of legislation, or actions of competitors). |

**Selection of risk treatment option**:

Selection the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived, with regard to legal, regulatory, and other requirements such as social responsibility and the protection of natural environment.

**Assessment of control effectiveness:**

The table below is used to assist management in the assessment of the perceived effectiveness of controls to mitigate or reduce the impact or likelihood of specific risks.

| RATING | FACTOR | CRITERIA |
|---|---|---|
| 81-90% | Highly effective | Controls are implemented and are highly effective |
| 61-80% | Effective | Controls are effective and implemented |
| 41-60% | Controls are adequate | Controls require improvements to be effective |
| 21-40% | Controls needs improvements | Controls not effective or adhered to |
| 0-20% | Controls not effective | Limited controls in place and major deficiencies |
| 0% | No Control | No Controls in place |

## CHAPTER 7

### 7.1 MONITORING AND ADVISORY

Risk Management Committee is responsible for reviewing, monitoring and reporting on risk profiles on a regular basis for management of exposures. This is done to ensure achievement of strategic/ operational goals and objectives. Risk Owners are responsible for management of identified risks towards acceptable levels.

The following aspect are to be considered during risk monitoring and review process:

- Implementation of the Action plans;
- Key Risk Indicators (KRIs) and associated Key Performance Indicator (KPIs); and
- New and emerging risks.
- Internal audit & external audit

## CHAPTER 8

### 8.1 COMMUNICATION AND REPORTING

The following outlines the reporting, stakeholders and action required for each type of report.

| REPORT | STAKEHOLDER | ACTION REQUIRED | FREQUENCY |
|---|---|---|---|
| Risk assessment report | Risk Owner and Top Management | • Implementation of the action plans and recommendations<br>• Recommend for approval | Annually and Quarterly |
| | • RMC<br>• AC | • Recommend for approval | Annually and Quarterly |
| | • Mayoral<br>• Council | • Noting<br>• Approval | Annually and Quarterly |
| Risk Management Statement in Annual Report | • Top Management<br>• Mayoral<br>• Council<br>• MPAC<br>• Council | • Input<br>• Recommend for approval<br>• Oversight<br>• Approval | Annually |
| | • External Parties<br>• Public | Information | Annually |
| Risk report | • Technical Clusters<br>• EMT & EEMT<br>• Sub-mayoral<br>• Mayoral<br>• GRGC<br>• Council | • Noting<br>• Noting<br>• Approval for mayoral consideration<br>• Noting<br>• Approval<br>• Noting | Monthly and Quarterly |
| Framework and Policies | • PDC<br>• Top Management<br>• RMC<br>• Audit Committee<br>• Mayoral<br>• Council | • Input<br>• Recommend for approval<br>• Approval<br>• Advise and recommend<br>• Recommends to Council<br>• Approval for implementation | Annually |

## 8.2 REPORTING TEMPLATE

**The following templates are attached as Annexures**

- Risk Registers
- Quarterly progress monitoring template

## 8.3 RISK MANAGEMENT FRAMEWORK REVIEW AND APPROVAL

The GGM Risk Management Framework must be reviewed as and when required within the cycle of 5 years.

Authority

**Signed By:**

**The Mayor** ______________________ 17\05\2024

**CLLR ZITHA T** **Signature** **Date**