KWADUKUZA MUNICIPALITY

ENTERPRISE-WIDE RISK MANAGEMENT FRAMEWORK

FINANCIAL YEAR: 2023/2024

TABLE OF CONTENTS

1. INTRODUCTION

The Framework has been developed in terms of sections 62(1) (c)(i) and 95(c)(i) of the MFMA, which require the Accounting Officers to ensure that their municipality have and maintain effective, efficient and transparent systems of risk management.

KwaDukuza Local Municipality 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 KwaDukuza Local Municipality strategic management. It is the process whereby the KwaDukuza Local Municipality 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 KwaDukuza Local Municipality will manage risks faced in an appropriate manner.

2. TERMS AND DEFINITIONS

BASIC TERMS	*DEFINITON*
General Terminology	
Risk	*The uncertainty of an event occurring that could have an impact on the achievement of objectives.* Note 1: Risk is a condition in which the possibility of loss exists Note 2: In some situations risk arises from the possibility of deviation from the expected outcome or event 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.
Consequence or Impact or Severity	Outcome of an **event** Note 1: There can be more than one consequence from one event Note 2: Consequences range from positive to negative. However, consequences are always negative for safety aspects Note 3: Consequencescan be expressed qualitatively or quantitatively
Probability	Extent to which the **event** is likely to occur 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 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

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

BASIC TERMS	*DEFINITON*
Cost of risk	Costs associated with: a) Insurance premiums b) Self retained losses (incurred loss) c) Loss control expenses including safety, security, property conservation, quality control programs, etc. d) 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
Interested Party	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
Risk Perception	Way in which a stakeholder views a risk based on a set of values or concerns Note 1: Risk perception depends on the **stakeholder's** needs, issues and knowledge Note 2: Risk perception can differ from objective data
Risk Communication	Exchange or sharing of information about **risk** between the decision-maker and other **stakeholders** Note : The information can relate to the existence, nature, form, probability, severity, acceptability, treatment or other aspects of risk

BASIC TERMS	*DEFINITON*
Terms Related to Risk Assessment	
Risk Assessment	Overall process of **risk analysis** and **risk evaluation** in order to identify potential opportunities or minimise loss. 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.)
Risk Analysis	Systematic use of information to identify **sources** and to estimate the **risk** Note1: Risk analysis provides a basis for **risk evaluation, risk treatment** and **risk acceptance.** Note 2: Information can include historical data, theoretical analysis, informed opinions, and the concerns of **stakeholders**
Risk Identification	Process to find, list and characterise elements of **risk** Note 1: Elements can include source or hazard, event, consequence and probability Note 2: Risk identification can also reflect the concerns of stakeholders
Source Identification	Process to find, list and characterise **sources** Note : In the context of safety, source identification is called hazard identification
Risk Driver	The technical, programmatic and supportability facets of risk.
Risk Estimation	Process used to assign values to the **probability** and **consequences** of a **risk** Note : Risk estimation can consider cost, benefits, the concerns of **stakeholders** and other variables, as appropriate for **risk evaluation**

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

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

BASIC TERMS	*DEFINITON*
Enterprise Risk Manager (ERM) / Process Owner	An official of the Municipality who has no *other* responsibilities except for advising on, formulating, overseeing and managing all aspects of an organisation's **risk management system** 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.
Process Champion	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 **ERM** is provided with the necessary resources, capabilities and authority in order to fulfil the requirements of the Risk Management Framework.
Risk Officers/Champions	The risk officers assist the **ERM** in the fulfilment of their duties. These persons can be in line management in the departments but have an alternative reporting line to the **ERM** or report directly to the **ERM**.
Risk Matrix	The numbers of levels of probability and consequences chosen against which to measure risk.
Risk Profile	The Municipality has an **inherent** and **residual** risk profile. These are all the risks faced by the Municipality, ranked according to a **risk matrix** and indicated graphically on a matrix. The Risk Score is determined by multiplying the frequency and severity of the risk.
Risk Appetite	The level of **residual risk** that the organisation is prepared to accept without further **mitigation** 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
Risk Register	A formal listing of risks identified, together with the results of the **risk analysis, risk evaluation** procedures together with details of **risk treatment, risk control, risk reduction** plans
Key Risks	Risks which the organisation perceives to be its most significant risks
Key Risk Indicators	Indicators by which key risks can be easily identified
Risk Tracking	The monitoring of key risks over time to determine whether the level of risk is changing.

3. THE PURPOSE OF THE ENTERPRISE RISK MANAGEMENT (ERM) FRAMEWORK

3.1 Background or ERM

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.

This framework sets out the principles to support effective risk management. 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 IV), 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.***

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

a) 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.

b) Advance the development and implementation of modern management practices and to support innovation;

c) 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:

(i) Support KwaDukuza Local Municipality 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;

(ii) 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;

(iii) 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

(iv) Enhance stewardship and transparency by strengthening public sector capacity to safeguard human resources, property and interests.

4. BENEFITS OF THE ERM FRAMEWORK

The benefits of the Enterprise Risk Management Framework in KwaDukuza Local Municipality are as follows:

a) Aligning risk appetite and strategy – KwaDukuza Local Municipality Management considers their risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks.

b) 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.

c) 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 municipality.

d) Enhancing risk response decisions – ERM provides the rigor for management to identify and select among alternative risk responses – risk avoidance, reduction, sharing, and acceptance.

e) Reducing operational surprises and losses – KwaDukuza Local Municipality gains enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses.

f) Identifying and managing multiple and cross-enterprise risks – KwaDukuza Local 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.

g) Seizing opportunities – By considering a full range of potential events, management is positioned to identify and proactively realize opportunities.

h) Improving deployment of capital – Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation.

i) Ensuring compliance with laws and regulations – ERM helps ensure effective reporting and compliance with laws and regulations, and helps avoid damage to the municipality's reputation and associated consequences

j) Increasing probability of achieving objectives – ERM assists management in achieving KwaDukuza Local Municipality'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 fulfil its intentions to stakeholders.

The municipality shall adopt a policy statement which makes reference to this framework.

5. LEGAL MANDATE

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

5.1 Accounting Officer/Authority

According to section 62(1) (c) (i) of the Municipal Finance Management Act, 2003:
"The accounting officer of a municipality is responsible for managing the financial administration of the municipality, and must for this purpose take all reasonable steps to ensure that the municipality has and maintains effective, efficient and transparent systems of financial and risk management and internal control"

5.2 Management, Chief Risk Officer, Risk Champions and other personnel

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.

5.3 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 –

Prepare a risk based audit plan and an internal audit program for each financial year;

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".

a) 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;

(i) Effectiveness and efficiency of operations;

(ii) Safeguarding of assets; and

(iii) 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."

5.4 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 –

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"

5.5 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.

5.6 Corporate governance guidelines

KwaDukuza Local Municipality is encouraged to adhere to the principles espoused in the King Report on Corporate Governance (King IV). King IV discusses the following principles, which have been incorporated in this framework:

a) Responsibility for the governance of risk;
b) The determination of risk tolerance;
c) The establishment of a risk management committee;
d) The responsibility of management to design, implement and monitor the risk management plan;

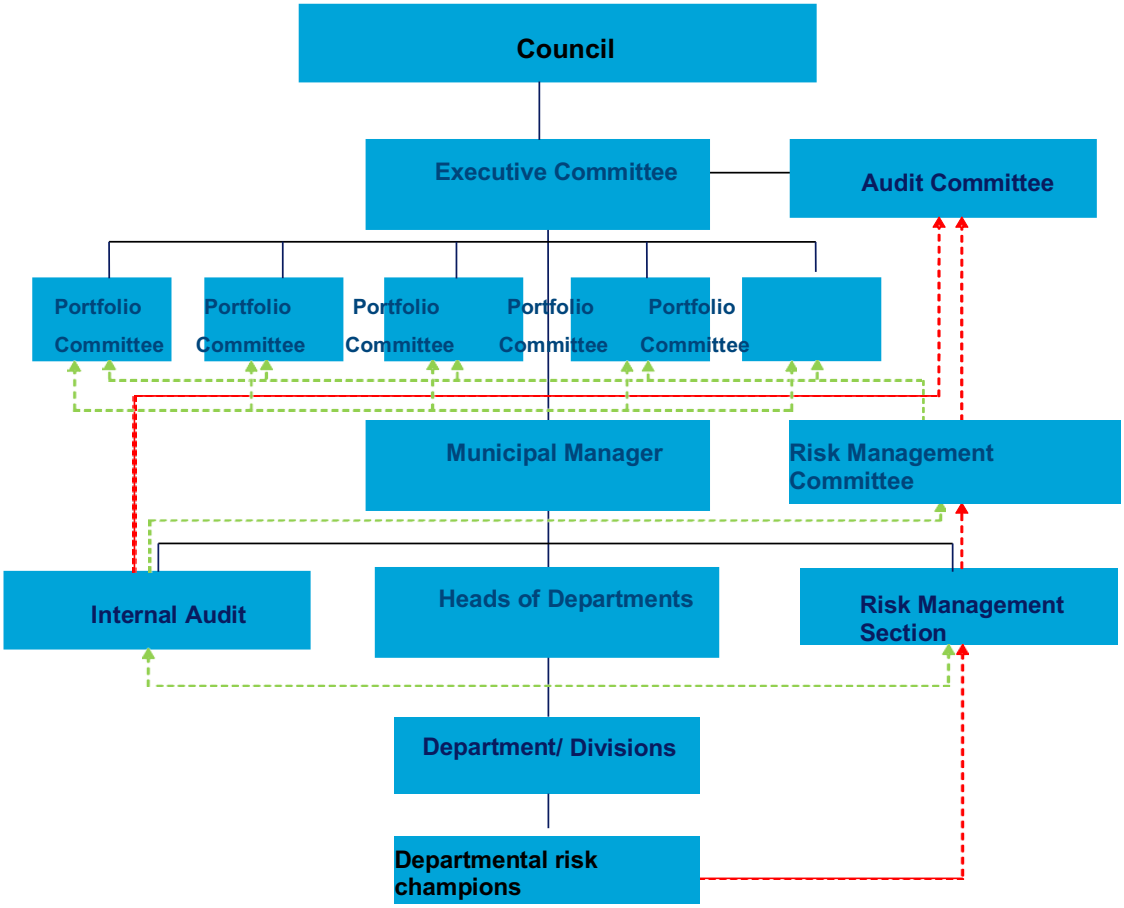
e) The performance on continuous risk assessments;
f) The implementation of frameworks and methodologies;
g) The implementation of appropriate risk responses by management;
h) The implementation of continuous risk monitoring by management; and
i) Assurance to be provided on the effectiveness of the risk 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.

6. MUNICIPAL RISK MANAGEMENT OVERSIGHT STRUCTURE

A risk management reporting and communication structure should be implemented to ensure oversight and accountability for enterprise risk management.

KwaDukuza Local Municipality Risk Management Oversight structure is as follows:



→	Risk reporting
→	Risk information flows
→	Administrative reporting

7. ROLES, RESPONSIBILITIES AND GOVERNANCE

a) The Accounting Officer of the municipality/ municipal entity is ultimately responsible for ERM and should assume overall ownership.

b) All managers and employees have some responsibility for ERM.

c) Managers support the risk management philosophy, promote compliance with the risk appetite and manage risks within their spheres of responsibility consistent with risk tolerances.

d) Personnel are responsible for executing ERM in accordance with established directives and protocols.

e) A number of external parties often provide information useful in effecting ERM, but they are not responsible for the effectiveness of the KwaDukuza Local Municipality's ERM processes and activities.

7.1 Members of Council

Councillors are collectively accountable for the achievement of the goals and objectives of the KwaDukuza Local Municipality. 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.
The council may delegate this responsibility to an Executive Committee of the Council.

High level Risk Management responsibilities of the Council are as follows:

a) Providing oversight and direction to the municipality on the risk management related strategy and policies;
b) Having knowledge of the extent to which the municipality and management has established effective risk management and assign responsibility & authority;
c) Awareness of and concurring with the municipality's risk appetite and tolerance levels;
d) Reviewing the municipality's portfolio view of risks and considering it against the risk tolerance;
e) Influencing how strategy and objectives are established, municipal activities are structured, and risks are identified, assessed and acted upon;
f) Requiring that management should have an established set of values by which every employee should abide by;
g) Insist on the achievement of objectives, effective performance management, accountability and value for money.

Consideration of:

(i) The design and functioning of control activities, information and communication systems, and monitoring activities;
(ii) The quality and frequency of reporting;
(iii) The way the municipality is managed including the type of risks accepted;
(iv) The appropriateness of the reporting lines

7.2 Accounting Officer/ Municipal Manager

The Accounting Officer is accountable for the municipality's risk management in terms of legislation. It is important that the Accounting Officer sets the right tone for risk management in the municipality, this will ensure that the municipality operates in a conducive control environment where the overall attitude, awareness, and actions of management regarding internal controls and their importance to the municipality is at par with the stated vision, values and culture of the municipality. Accounting officer establishes the right tone for the prevention and management of fraud and misconduct in the municipality. This is achieved through the developing and publishing a fraud and misconduct risk management policy.

Accounting Officer is responsible for:

a) the identification of key risks facing the municipality;
b) the total process of risk management, which includes a related system of internal control;
c) for forming opinion on the effectiveness of the process;
d) providing monitoring, guidance and direction in respect of ERM;
e) ascertaining the status of ERM within the municipality, by discussion with senior management and providing oversight with regard to ERM by:
f) Knowing the extent to which management has established effective ERM;
g) Being aware of and concurring with the set risk appetite;
h) Reviewing the institution's portfolios view of risk and considering it against respective risk appetite; and
i) Considering the most significant risks and whether management is responding appropriately
j) Identifying and fully appreciating the risk issues and key risk indicators affecting the ability of the municipality to achieve its strategic purpose and objectives;
k) 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 municipal assets and reputation are suitably protected;
l) Ensuring that the municipality's ERM mechanisms provides an assessment of the most significant risks relative to strategy and objectives;
m) Considering input from the internal auditors, external auditors, auditor general, risk committee and subject matter advisors regarding ERM;
n) 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;
o) For Enterprise Risk Management disclosures in the annual report;
p) 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;
q) Hold management accountable for designing, implementing, monitoring and integrating risk management principles into their day-to-day activities.

7.2 Risk Management Committee (Anti-Fraud and Corruption/ Ethics/ Loss Prevention/ Business Continuity)

The Risk Management Committee is an oversight committee responsible to the Accounting Officer for the monitoring of risk management. It is responsible for assisting the Accounting Officer in addressing its oversight requirements of risk management and evaluating the municipality'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 municipality.

At KwaDukuza Local Municipality, Risk Management Committee has been established and chaired by an independent person.

The responsibilities of the Risk Management Committee may include:

a) Review the risk management policy and strategy, and recommend for approval by the Accounting Officer;
b) Review and assess the integrity of the risk control systems and ensure that the risk policies and strategies are effectively managed;
c) Set out the nature, role, responsibility and authority of the risk management / risk officer function within the municipality and outline the scope of risk management work;
d) Monitor the management of significant risks to the municipality, including emerging and prospective impacts;
e) Review any legal matters, together with the legal advisor, that could have a significant impact on the municipality;
f) Review management and internal audit reports detailing the adequacy and overall effectiveness of the municipality'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;
g) Review risk identification and assessment methodologies to obtain reasonable assurance of the completeness and accuracy of the risk register;
h) Review and approve the risk tolerance for the municipality;
i) Evaluate the effectiveness of mitigating strategies to address the material risks of the municipality;
j) Report to the Accounting Officer any material changes to the risk profile of the municipality;
k) Review and approve any risk disclosures in the Annual Financial Statements;
l) 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;
m) Monitor progress on action plans developed as part of the risk management process;
n) 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;
    (i) 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;

(ii) 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;

o) Providing feedback to the audit committee on the effectiveness of risk management;
p) Develop goals, objectives and key performance indicators of the Committee for approval by the Accounting Officer;
q) Develop goals, objectives and key performance indicators to measure the effectiveness of the risk management activity;
r) Set out the nature, role, responsibility and authority of the risk management function within the municipality for approval by the Accounting Officer, and oversee the performance of the risk management function;
s) 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.
t) ensure the implementation of the anti-fraud and corruption strategy,
u) create fraud awareness amongst all stakeholders.
v) accept responsibility for considering any reports of fraud or misconduct and
w) take appropriate action in consultation with the Accounting officer.
x) Review Loss Prevention and Control Policy and recommend for approval by the Accounting Officer and Council.
y) Monitor of the application of the Loss Prevention and Control Policy;

z) Evaluate the effectiveness of the implementation of the Loss Prevention and Control Policy;

aa) Review the process implemented by management in respect of loss prevention and control and ensures that all losses are followed up appropriately;

bb) Ensure that the reports of losses are followed up and the losses and claims register is updated;

cc) Provide quarterly reports to the Audit Committee that summarises the Municipality's loss prevention, control and action for the period.

7.3.1 The Risk Management Committee, in fulfilling its role, is responsible for ensuring that the following is achieved:

a) Monitoring of the application of the anti-fraud policy and ensuring adequate supervision and dynamism of the controls and procedures.
b) The planned and required activities are undertaken such as the policy inclusion in the letter of appointment for staff, communication and training campaigns.
c) Review the fraud prevention policy and recommend for approval by the Accounting Officer;

d) Evaluate the effectiveness of the implementation of the fraud prevention policy;
e) Reviews the process implemented by management in respect of fraud prevention and ensures that all fraud related incidents have been followed up appropriately.
f) An appropriate fraud risk assessment is completed.
g) The reports of fraud and misconduct are effectively handled.
h) Consistent and appropriate action is taken on known incidents of fraud and misconduct.
i) Quarterly reports to the Audit Committee that summarises the municipality's fraud prevention, detection and action for the period.

7.4 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 municipality. 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:

a) designing an ERM programme in conjunction with the Chief Risk Officer;
b) deciding on the manner in which risk mitigation will be embedded into management processes;
c) inculcating a culture of risk management in the municipality ;
d) providing risk registers and risk management reports to the Chief Risk Officer pertaining to risk and control;
e) identifying positive aspects of risk that could evolve into potential opportunities for the municipality by viewing risk as an opportunity by applying the risk/reward principle in all decisions impacting upon the municipality;
f) assigning a manager to every key risk for appropriate mitigating action and determining an action date;
g) holds official accountable for their specific risk management responsibilities;
h) utilising available resources to compile, develop and implement plans, procedures and controls within the framework of the municipality's Enterprise Risk Management Policy to effectively manage the risks within the municipality;
i) ensuring that adequate and cost effective risk management structures are in place;
j) identifying, evaluating and measuring risks and where possible quantifying and linking each identified risk to key risk indicators;
k) 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;
l) implementation of cost effective preventative and contingent control measures
m) implementation of procedures to ensure adherence to legal and regulatory requirements;
n) monitoring of the ERM processes on both a detailed and macro basis by evaluating changes, or potential changes to risk profiles;

o) implementing and maintaining adequate internal controls and monitoring the continued effectiveness thereof;
p) 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;
q) reporting to the Audit Committee on the risk process and resultant risk/ reward profiles;
r) defining the risk management roles, responsibilities and accountabilities at senior management level.

7.5 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 municipality'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:
(i) constitution;
(ii) membership;
(iii) authority;
(iv) terms of reference; and
(v) meetings.

The Audit Committee further:

a) Reviews written reports furnished by the Risk Management Committee detailing the adequacy and overall effectiveness of the Risk Committee's function and its implementation by management.
b) 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 municipality.
c) Ensure that risk definitions and contributing factors, together with risk policies, are formally reviewed on an annual basis.
d) Review the acceptability of the risk profile in conjunction with the overall risk appetite of the municipality, taking into account all risk mitigation factors, including, but not limited to, internal controls, business continuity and disaster recovery planning, etc.
e) Ensure compliance with the risk policy and framework.

f) Oversee that the Risk Management Committees of the municipality is operating effectively;
g) Receive and consider periodic reports (quarterly) on the activities of the Enterprise Risk Management Committees.
h) 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 municipality, have been identified during the risk assessment process. This includes an awareness of emerging risks pertaining to the municipality.
i) Facilitates and monitors the coordination of all assurance activities implemented by the municipality.
j) Reviews and recommends any risk disclosures in the annual financial statements;
k) Provides regular feedback to the Accounting Officer on the effectiveness of the risk management process implemented by the municipality.
l) Reviews and ensures that the internal audit plans are aligned to the risk profile of the municipality.
m) Reviews the effectiveness of the internal audit assurance activities and recommends appropriate action to address any shortcomings.

7.6 Executive Directors

Executive Directors in charge of municipal departments have overall responsibility for managing risks related to their objectives and are responsible for:

a) Identifying, assessing and responding to risk relative to meeting their department's objectives;
b) Ensuring that the processes utilised are in compliance with the municipality's Enterprise Risk Management policies and that their activities are within the established risk tolerance limits;
c) Reporting on progress and issues to the municipality's Enterprise Risk Manager;
d) Complying with Enterprise Risk Management policies and developing techniques tailored to the department's activities;
e) applying ERM techniques and methodologies to ensure risks are appropriately identified, assessed, responded to, reported on and monitored;
f) ensuring that risks are managed on a daily basis; and
g) providing leadership with complete and accurate reports regarding the nature and extent of risks in the department's activities.

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

7.7 Chief Risk Officer (CRO)

The primary responsibility of the Chief Risk Officer is to bring his / her specialist expertise to assist the municipality 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 Enterprise Risk Management approach.

Responsibilities of the Chief Risk Officer include:

a) Working with Senior Managers 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;
b) Undertakes a Gap Analysis of the municipality's ERM process at regular intervals;
c) Performs reviews of the risk management process to improve the existing process;
d) 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.;
e) Develops systems to facilitate risk monitoring and risk improvement;
f) Ensures that all risk categories are included in the assessment;
g) Ensures that key risk indicators are included in the risk register;
h) Aligns the risk identification process with the municipality's targets and objectives;
i) Agrees on a system of risk quantification;
j) Identifies relevant legal and regulatory compliance requirements;
k) Compiles a consolidated risk register on an annual basis;
l) Costs and quantifies actual non-compliance incidences and losses incurred and formally reports thereon;
m) Formally reviews the occupational health, safety and environmental policies and practices;
n) Consolidates all information pertaining to all risk related functions, processes and activities;
o) Reviews the Business Continuity Management Plans;
p) Liaises closely with the Internal Audit to develop a risk based audit plan and management assurance plans,
q) Benchmarks the performance of the municipality's risk management process to other entities both nationally and internationally;
r) Assist in compiling risk registers for all functional areas at strategic, tactical and operational levels;
s) Communicates the risk strategy to all management levels and to employees;
t) Ensures that the documentation is developed in respect of the risk management process;
u) Communicates with the Provincial Treasury, Audit Committee and the Risk Management Committee regarding the status of ERM;
v) Regularly visits functional areas and meets with senior managers to promote embedding risk management into the culture and daily activities of the institution;
w) Works with leaders to ensure that municipal plans and budgets include risk identification and management;
x) Compiling the necessary reports to the Risk Management Committee;

y) 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.
z) Review Loss Prevention and Control Policy and recommend for approval by the Accounting Officer and Council.
aa) Monitor of the application of the Loss Prevention and Control Policy;
bb) Evaluate the effectiveness of the implementation of the Loss Prevention and Control Policy;
cc) Ensure processes are implemented on loss prevention and control and ensures that all losses are followed up appropriately;
dd) Ensure that the reports of losses are followed up and the losses and claims register is updated; and
ee) Provide quarterly reports to the Audit Committee that summarises the Municipality's loss prevention, control and action for the period.

7.8 Risk Champions

The duties of the Risk Champions shall be:

a) Co-ordinate the Risk Management Activities (Risk Management; Anti-fraud and Corruption; Ethics Risk management) of their departments;
b) Report to the Enterprise Risk Management unit of any material changes to the risk profile of the department;
c) Provide proper and timely reports to Enterprise Risk Management unit on the state of risk management, Anti-fraud and Corruption and Ethics Risk management together with aspects requiring improvement accompanied by the Forum's recommendations to address such issues.
d) Discuss and incorporate risks that cut across the departments and the organizational risk registers into their departmental risk registers;
e) Intervene in instances where the risk management efforts are being hampered, for example, by the lack of co-operation by Management and other officials and lack of institutional skills and expertise;
f) Provide input on the impact from the knowledge of operational risks into the improvement of the strategic risk profile of the municipality.
g) Attend at all risk management and related activities of the organization (Risk Management; Anti-fraud and Corruption; Ethics Risk management)

7.9 Internal Audit

Internal Audit is accountable to the Accounting Officer for providing independent assurance regarding the risk management activities of the municipality. Hence, Internal Audit is responsible for providing independent assurance that management has identified the municipality's risk and has responded effectively.

Internal Audit is responsible for:

a) Reviewing the risk philosophy of the municipality. This includes the risk management policy, risk management strategy, fraud prevention plan, loss prevention and management policy, risk management reporting lines, the values that have been developed for the municipality;

b) Reviewing the appropriateness of the risk tolerance levels set by the municipality taking into consideration the risk profile of the municipality;
c) Providing assurance over the design and functioning of the control environment, information and communication systems and the monitoring systems;
d) Providing assurance over the municipality's risk identification and assessment processes;
e) Utilising the results of the risk assessment to develop internal audit plans;
f) Providing independent assurance as to whether the risk management strategy, risk management implementation plan and fraud prevention plan have been effectively implemented within the municipality;
g) 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.

7.10 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:

a) The reasonability of the financial statements; and
b) Compliance with applicable legislation

In addition,

(i) 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,

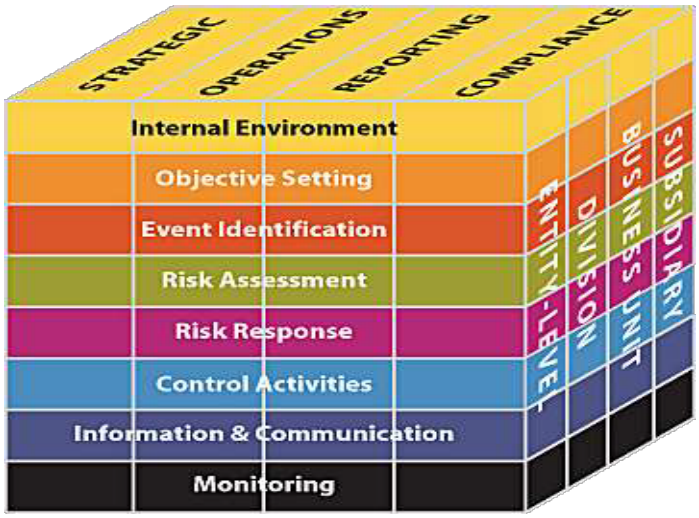
(ii) the Auditor- General will provide independent assurance on the effectiveness of the risk management activities.

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

(iv) 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 for the purposes of effective financial reporting and management of risk.

8. ENTERPRISE RISK MANAGEMENT (ERM) APPROACH

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

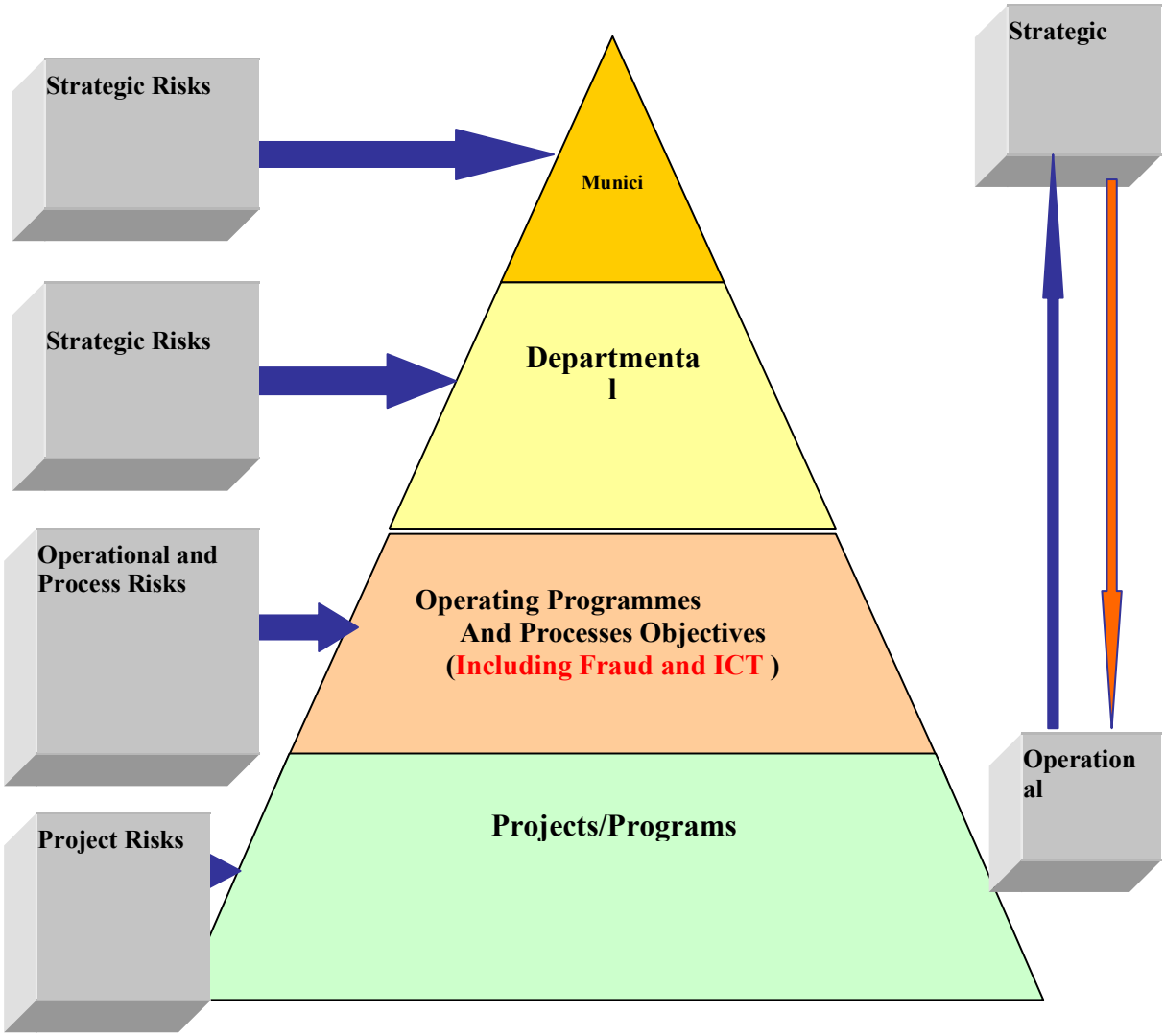


The implementation of enterprise-wide risk management is guided by the methodology outlined in this document. The methodology allows for a consistent approach to be applied within the municipality.

8.1 Risk Profiles

Risk profile shall be developed and reviewed on an annual basis. Five levels of risk profiles need to be developed and maintained by the municipality. These are:

a) Strategic,
b) Operational;
c) Process;
d) Project and
e) Occupational Health and Safety



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

8.1.1 Strategic level

a) 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;
b) 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;
c) 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;

d) strategic risk assessment should be updated during the annual review of the Integrated Development Plan and budgetary processes;
e) 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;
f) 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.

8.1.2 Operational level

a) operational risk identification should seek to establish vulnerabilities introduced by employees, internal processes and systems, contractors, regulatory authorities and external events;
b) operational risk assessments should be performed during the annual departmental planning and budgeting processes, and be continually monitored for new and emerging risks;
c) specific operational risk assessments may need to be performed in certain areas using specialist skills, such as fraud risk assessments (refer 5.3 below), information technology risk assessments, compliance risk assessments and safety and health risk assessments; etc
d) 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;
e) 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.

8.1.3 Process level

a) process risk identification should seek to establish risks to the achievement of the specific process objectives;
b) 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;
c) 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.

8.1.4 Program / Project level

a) this involves the identification of risks inherent to particular programs and projects;
b) risks should be identified for all major projects, covering the whole project lifecycle;

c) it is aimed to facilitate risk owners in ensuring that adequate and effective strategies and controls are implemented and monitored throughout the project lifecycle;
d) risks documented in project risk register, monitored and regularly reviewed to identify new and emerging risks.

8.2 Developing risk profiles

8.2.1 Risk Identification

a) 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 organisation's key risks.

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

c) 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.

d) 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.

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

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

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

(i) Risk identification should be strengthened by:
(ii) Review of internal and external audit reports;
(iii) Financial analyses;
(iv) Historic data analyses;
(v) Actual loss data;
(vi) Interrogation of trends in performance data;
(vii) Benchmarking against peer groups;
(viii) Market and sector information;
(ix) Scenario analyses; and
(x) Forecasting and stress testing

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

TECHNIQUE	ADVANTAGES	DISADVANTAGES
Individual Interview	✓ 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.
Workshops	✓ 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.
A Combination of the Above	✓ 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.
Staff Surveys	✓ 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.
Selected Groupings	✓ 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.

8.2.2 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. Risk Correlation will be done.

RISK CATEGORIES	DEFINITION OF RISK CATEGORIES
1. Strategic and service delivery risks	✓ 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
2.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.
2. Intergovernmental and Interdepartmental Co-ordination Risks	✓ 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
3. Governance, Compliance/ Regulatory and Reputational Risks	✓ Values and ethics, transparency, policies, procedures and processes as well organisational structures. ✓ 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. ✓ The reputation risks exposures are 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.
4. Political Risks	✓ *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.* ✓ *Risks emanating from political factors and decisions that have an impact on the institution's mandate and operations. Possible factors to consider include:* ➢ *Political unrest;* ➢ *Political instability;*

	➢ *Coalition;* ➢ *Local, Provincial and National elections; and* ➢ *Changes in office bearers.*
5. Economic Risks	Risks relating to ✓ *emerging or movements in the international, national, provincial markets and globalisations* Factors to consider include: ✓ *Inflation;* ✓ *Foreign exchange fluctuations;* ✓ *Interest rate &* ✓ *Load shedding*
6. Environmental Risks	Risks relating to ✓ *natural disasters as flood, fire or earthquake, and* ✓ *sustainable development.* ✓ *Noncompliance with environmental legislation* ✓ *Climate change* ✓ *Depletion of natural resources;* ✓ *Environmental degradation;* ✓ *Spillage; and Pollution*
7. Social Risks	Risks relating to ✓ *poverty alleviation,* ✓ *changing demographics,* ✓ *shifting of family structures,* ✓ *work/life priorities,* ✓ *social trends,* ✓ *unemployment* ✓ *level of citizen engagement.*
8. Infrastructure and Public Amenities Risks	Risks relating to infrastructure e.g. roads, buildings, etc. ➢ *Condition* ➢ *Shortage* ➢ *Maintenance* ➢ *Illegal usage* ➢ *Destruction and vandalism*
9. Financial Risks	✓ 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: ➢ *Cash flow adequacy and management thereof;* ➢ *Financial losses;* ➢ *Wasteful expenditure;* ➢ *Budget allocations;* ➢ *Financial statement integrity;* ➢ *Revenue collection; and* ➢ *Increasing operational expenditure*
10. Occupational Health and Safety.	✓ Risks arising from outbreak of diseases and pandemic. ✓ Risks that is associated with the safety and security of the communities as well as the execution of institutional mandate. ✓ Security of networks, systems and information.

	✓ Risk of unsafe working conditions
11. Human Resources	Risks associated with staff capacity in relation to: ➢ *Integrity and honesty;* ➢ *Recruitment;* ➢ *Skills and competence;* ➢ *Employee wellness;* ➢ *Employee relations;* ➢ *Retention;* ➢ *Non-familiarity of staff with the set guidelines and procedures, and* ➢ *Occupational health and safety* ➢ *Diversity Management and inclusion*
12. Technological and System Risks	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:* ✓ *Security of networks systems and information concerns;* ✓ *Technology availability (uptime);* ✓ *Applicability of IT infrastructure;* ✓ *Integration / interface of the systems;* ✓ *Effectiveness of technology; and* ✓ *Obsolescence of technology.*
13. Process/operational	✓ Ineffective and inefficient processes. ✓ Inadequate controls in the operational processes.
14.Program/ Project risks	Risks associated with ✓ *not meeting program/project scope, costs, duration and deliverables*
15. Fraud and Corruption Risks	These risks relate to ✓ *illegal or improper acts by employees resulting in a loss of the institution's assets or resources.* ✓ *Misappropriation* ✓ *Mile administration* ✓ *Theft* ✓ *Scams*
16. Organisational Cultural	Risks relating ✓ *to an institution's overall culture and control environment.* The various factors related to organisational culture include: ✓ *Communication channels and the effectiveness;* ✓ *Cultural integration;* ✓ *Entrenchment of ethics and values;* ✓ *Goal alignment; and* ✓ *Management style.* ✓ *Diversity management*

17. Disaster Recovery/ Business Continuity	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: ✓ *Disaster management procedures; and* ✓ *Contingency planning.*
18. Knowledge and information management	Risks relating to ✓ *an institution's management of knowledge and information.* In identifying the risks consider the following aspects related to knowledge management: ✓ *Availability of information;* ✓ *Stability of the information;* ✓ *Integrity of information data;* ✓ *Relevance of the information;* ✓ *Retention and* ✓ *Safeguarding* ✓ *Compliance with POPI Act*
19. Litigation	✓ Risks that the institution might suffer losses due to litigation and lawsuits against it. ✓ Losses from litigation can possibly emanate from claims by employees, the public, service providers and other third party; ✓ Failure by institution to exercise certain rights that is to its advantage.
20. Material resources (Procurement risk)	Risks relating to an institution's material resources. Possible aspects to consider include: ✓ *Availability of material;* ✓ *Costs and means of acquiring / procuring resources* ✓ *The wastage of material resources.*
21. Third party performance	✓ 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: ✓ *Outright failure to perform;* ✓ *Not rendering the required service in time;* ✓ Not rendering the correct service; and ✓ Inadequate / poor quality of performance.

8.2.3 Risk Assessment

a) 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.

b) 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.

c) 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:

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

d) 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.

8.2.3.1 Inherent and Residual Risk

a) 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.

b) 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.

c) 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.

d) 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.

8.2.3.2 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.

8.2.3.3 Control

Control is any action that has been put in place to mitigate the risk. A control could be a policy, procedure, 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.

8.3 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, the municipality 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.

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

Step 1: Estimating likelihood and impact

a) 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.
b) The likelihood of occurrence must be assessed for every identified risk.
c) Estimates of risk likelihood often are determined using data from past observable events, which may provide a more objective basis than entirely subjective estimates.
d) 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 municipality

Measures of likelihood of occurrence: Table of likelihood parameters

LIKELIHOOD TABLE

Likelihood Category	Category definition	Rating
Certain	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 in quantifying the potential impact that a risk exposure may have on the institution.

IMPACT TABLE

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

Severity ranking	Continuity of service delivery	Safety & Environmental	Technical complexity	Financial	Achievement of objectives	Rating
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 should be used to assist management in quantifying the inherent risk (i.e. pre controls)

Inherent risk exposure	Risk index value
Critical	≥50
Major	≥35 < 50
Moderate	≥25 < 35
Minor	≥15 < 25
Insignificant	< 15

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.

SEVERITY RANKING	RATING	ACTION AND REPORTING
Critical	100	Business Continuity plan be developed and Risks be reported to Audit Committee, Risk Management Committee and EXCO
Major	70	Business Continuity plan be developed and Risks be reported to Audit Committee, Risk Management Committee and EXCO

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

Risk appetite

a) 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.

b) 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.

c) 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:
   (i) the likelihood and impact of the risk could be so low that specific treatment is inappropriate
   (ii) the risk being such that no treatment is available
   (iii) 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 KwaDukuza Local Municipality'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 KwaDukuza Local Municipality 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 KwaDukuza Local Municipality will be reflected in the risk rating scales used to assess the risks.

Step 4. Considering the Risk Response

a) 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.

b) 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:

(i) **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.

(ii) **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.

(iii) **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.

(iv) **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.

c) 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 line within the risk appetites, while an acceptance response suggests that inherent risk is already in line with risk appetites.

d) 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:

(i) Evaluating the effectiveness of existing measures on reducing the risk to an acceptable level.

(ii) 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.

(iii) Assessing the costs versus benefits of potential risk responses.

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

a) 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.

b) 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.

c) 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.

d) 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.

e) 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 threating 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.

CONTROLS TABLE

EFFECTIVENESS CATEGORY	CATEGORY DEFINITION	RATING
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 TABLE

Residual risk exposure	Risk acceptability	Proposed actions	Factor	Monetary Quantification	Monitoring Level
Critical	Unacceptable	Take action to reduce risk with highest priority, accounting officer/chief executive officer and executive authority/accounting authority attention.	≥25	≥5% of Budget or Income	✓ Manco, ✓ Risk Management Committee, ✓ Audit Committee, EXCO ✓ Portflolio Committees
Major	Unacceptable	Take action to reduce risk with highest priority, accounting officer/chief executive officer and executive authority/accounting authority attention.	≥15 < 25	≥4% <5% of Budget or Income	✓ Manco, ✓ Risk Management Committee, ✓ Audit Committee, EXCO ✓ and Portflolio Committees

Moderate	Unacceptable	Take action to reduce risk, inform senior management.	≥7.5 < 15	≥3% <4% of Budget or Income	✓ MANCO, ✓ Risk Management Committee, ✓ Audit Committee,
Minor	Acceptable	No risk reduction - control, monitor, inform management.	≥7.5 < 2.5	2.5% <3%of Budget or Income	✓ MANCO, ✓ Risk Management Committee.
Insignificant	Acceptable	No risk reduction - control, monitor, inform management.	< 2.5	2% of budget or income	✓ MANCO

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.

ACTIONS TO MITIGATE RISK EXPOSURE

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 ✓ No actions required due to non ✓ availability of resources
Yellow – Minor	Action within 6 months	✓ Review within 9 months ✓ No new actions required, Management implement and monitor actions to bring the risk within the appetite.
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

9. 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 will be based on the municipality's risk profiles, as follows:

a) Strategic
b) Operational (Including Fraud and Corruption and ICT)
c) Project specific (where there are such projects)

Risks will be reported quarterly as per table where impact is Level 3-5 to Risk Management Committee, Audit Committee, Portfolio Committees and EXCO. 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:

(i) Strategic and business objectives
(ii) Risk category
(iii) Risk name
(iv) Risk description (including root cause and consequence)
(v) Risk owner
(vi) Inherent risk rating
(vii) Risk Indicator
(viii) Control names for controls that mitigate the risk
(ix) Control descriptions (including whether it is a preventative, detective or corrective control)
(x) Control effectiveness rating
(xi) Residual risk ratings
(xii) Task information where identified - details, due dates and the accountable officials.
(xiii) Key Performance Indicator

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

10. COMBINED ASSURANCE

a) 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.

b) 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.

c) 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:

i. *The Office of the Auditor General,*
ii. *Internal Audit,*
iii. *Consulting engineers,*
iv. *Ethics' specialists,*
v. *Compliance and Legal specialists,*
vi. *Culture and climate surveys,*
vii. *Health and safety inspectors,*
viii. *Information security and*
ix. *Performance Monitoring and Evaluation Units*
x. *Provincial Departments.*
xi. *Statutory professional bodies*
xii. *Statutory compliance bodies.*
xiii. *Regulators. e. g. NERSA*

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 municipality. 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 of 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 Enterprise Risk Manager 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 Enterprise Risk Manager to facilitate, if necessary, a re-rating of the risk and incorporating the agreed management actions into the risk management tasks.

11. MONITORING

a) If existing controls are weak and exposes the municipal activities to risks, 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.

b) 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.

c) Management's performance with the processes of ERM will be measured and monitored through the following performance management activities:
   (i) monitoring of progress made by management with the implementation of the ERM methodology;
   (ii) monitoring of key risk indicators;
   (iii) monitoring of loss and incident data;
   (iv) management's progress made with risk mitigation action plans; and
   (v) *an annual quality assurance review of ERM performance.*

12. 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 the municipality, 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 will be considered when integrating ERM into municipality's decision making structures:

a) *Aligning risk management with objectives at all levels of the municipality;*
b) *Introducing risk management components into existing strategic planning and operational practices;*
c) *Communicating municipality's direction on an acceptable level of risk;*
d) *Including risk management as part of employees' performance appraisals and Business Units' annual operational plans; and*
e) *Continuously improving control and accountability systems and processes to take into account risk management and its result*

13. APPROVAL OF FRAMEWORK

The Risk Management Framework is approved by for implementation by KwaDukuza Municipality with effect from the 1st of July.

RECOMMENDED BY:

_____ _____

RISK MANAGEMENT COMMITTEE **DATE**

ADOPTED BY KDM COUNCIL:

_____ _____

COUNCIL RESOLUTION NO **DATE**