



**CITY OF EKURHULENI
Metropolitan Municipality**

EXTRACT FROM THE MINUTES OF THE ORDINARY COUNCIL MEETING OF THE CITY OF EKURHULENI METROPOLITAN MUNICIPALITY HELD ON THE 26 OCTOBER 2022

A-CORP (19-2022) CSSOC CORPORATE & SHARED SERVICES OVERSIGHT COMMITTEE REPORT ON THE RISK MANAGEMENT DEPARTMENT: REQUEST FOR COUNCIL TO APPROVE THE REVISED ENTERPRISE RISK MANAGEMENT POLICY

RESOLVED

- 1. That** the Corporate & Shared Services Oversight Committee Report on the Risk Management: Request for council to approve the revised Enterprise Risk Management Policy **BE NOTED.**
- 2. That the** Risk Management: Request for council to approve the revised Enterprise Risk Management Policy **BE APPROVED.**
- 3. That** the revised Enterprise Risk Management Policy attached as **Annexure A BE RECOMMENDED** for approval.

**CERTIFIED A TRUE EXTRACT
SIGNED AT GERMISTON ON THIS 16TH DAY OF JANUARY 2023**



SECRETARY OF COUNCIL: CITY OF EKURHULENI METROPOLITAN MUNICIPALITY

ANNEXURE A



**ENTERPRISE RISK
MANAGEMENT POLICY**

**DOCUMENT CLASIFICATION:
PUBLIC**

Title: **Enterprise Risk Management
Policy**

Document Identifier:

Alternative Reference
Number:

Area of Applicability: **City-Wide**

Functional Area:

Revision: **2**

Total Pages: **40**

Next Review Date: **2027**

Disclosure
Classification: **Controlled Disclosure**

Content

| | Page |
|--|------|
| 1. Introduction | 3 |
| 2. Policy/Directive Content | 3 |
| 3. Supporting Clauses | 4 |
| 3.1. Scope | 4 |
| 3.2. Normative/Informative References..... | 5 |
| 3.2.1. Normative..... | 5 |
| 3.2.2. Informative | 5 |
| 3.3. Definitions..... | 5 |
| 3.4. Abbreviations..... | 6 |
| 3.5. Roles and Responsibilities | 6 |
| 3.6. Process for Monitoring | 13 |
| 4. Acceptance | 13 |
| 5. Revisions | 14 |
| Annex A – Enterprise Risk Management Framework | 15 |

CONTROLLED DISCLOSURE

When downloaded from the document/knowledge management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, City of Ekurhuleni

1. Introduction

- 1.1. In the broadest sense, effective risk management ensures the continuity of municipal operations, and the maintenance of services to, and protection of the interests of, the City of Ekurhuleni (“CoE” or “City”) community. Due to the manner which risks are presented throughout municipal operations, the successful delivery of a program is contingent upon effective and cohesive management of those risks.
- 1.2. The importance of risk management has been growing steadily during the last several years. There is increasing awareness and expectation in the public sector of the need to manage risks, rather than leaving them solely to insurance.
- 1.3. The risk environment has been evolving rapidly, as advancing technological and social developments bring forth new or hitherto dormant risks associated with such phenomena as hazardous materials, pollution, electronic data, and exposure to legal and political liability. The municipality has an obligation to be fully aware of the state of the art in risk management, and to prevent losses and unnecessary expenditures.
- 1.4. Risk management can be extremely cost-effective when departments and municipal entities assess their risks properly and determine the most economical way to avoid them entirely, or reduce them to a minimum and limit potential expenditures arising from accidents or emergencies.
- 1.5. Risk management is a logical step-by-step process to protect, and consequently mitigate against uncertainty to the CoE’s property, interests and employees.
- 1.6. The Municipal Finance Management Act of 2003 (MFMA) and the King IV Report on Corporate Governance South Africa require the City, including municipal entities, to affect a process of Enterprise Risk Management (ERM) and as such the Council has established this process. The ERM function was established to position the City to mitigate any material risk through a system of knowledge and planned controls. The municipality has developed and will implement an ERM system that will ensure that the City’s business risks are identified and effectively managed on a continual basis.

2. Policy/Directive Content

2.1. Policy Statement

- 2.1.1. The City regards Enterprise Risk Management (ERM) as a critical cornerstone of good corporate governance and essential for the reasonable assurance on the achievement of its objectives when faced with uncertainty.
- 2.1.2. To this end all uncertainties that may prevent the City from achieving its business objectives shall be:
 - i. Proactively identified and formally assessed;
 - ii. Prioritised;
 - iii. Responded to;
 - iv. Reported on to relevant stakeholders; and

CONTROLLED DISCLOSURE

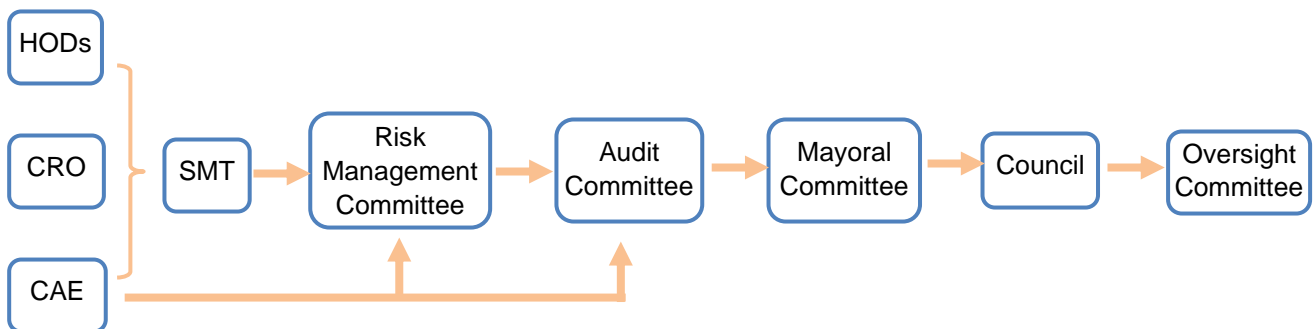
- v. Monitored to provide greater assurance of the achievement of these.

2.1.3. Uncertainty/risks shall be managed formally and proactively through a factual approach to decision-making, based on the logical and intuitive analysis of data and information collected about those risks.

2.1.4. In support of this policy, the City shall maintain an Enterprise Risk Management Framework that provides the methodology and processes to be followed in implementing risk management.

2.2. Policy Principles or Rules

2.2.1. The channels for the reporting of risk information are as prescribed in the diagram below, in line with the roles and responsibilities defined in this policy.



3. Supporting Clauses

3.1. Scope

This policy relates to Enterprise Risk Management

3.1.1. Purpose

The purpose of this policy is to outline the City of Ekurhuleni’s intent and position on Enterprise Risk Management.

3.1.2. Applicability

This policy shall apply throughout the City of Ekurhuleni. Municipal entities shall adopt the principles contained in this policy for group alignment.

CONTROLLED DISCLOSURE

3.2. Normative/Informative References

Persons using this document shall apply the most recent edition of the documents listed in the following paragraphs.

3.2.1. Normative

Not applicable

3.2.2. Informative

- i. The King IV Report on Corporate Governance for South Africa, 2016 by King Committee on Corporate Governance. The Institute of Directors in South Africa: Johannesburg.
- ii. Municipal Finance Management Act, Act No. 56 of 2003.
- iii. Municipal Structures Act, Act No. 117 of 1998.
- iv. Municipal Systems Act, Act No. 32 of 2000.
- v. Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2017, Enterprise Risk Management Integrated Framework.
- vi. International Organization for Standardization. ISO 31000:2018
- vii. Risk Management Standard Public Sector Risk Management Framework: National Treasury.

3.3. Definitions

| | Term | Definition |
|------|-----------------------|---|
| i. | Accounting Officer | The accounting officer of the municipality is the municipal manager, in terms of section 60 of the Municipal Finance Management Act. |
| ii. | Chief Audit Executive | The head of the Internal Audit department |
| iii. | Chief Risk Officer | The head of the Risk Management Department |
| iv. | City of Ekurhuleni | The municipality referred to as the Ekurhuleni Metropolitan Municipality. The term "City" is used interchangeably with "City of Ekurhuleni". |
| v. | Council | The council of a municipality is the structure referred to in section 18 of the Municipal Structures Act |
| vi. | Mayoral Committee | The mayoral committee is a structure established in terms of section 60 of the Municipal Structure Act. It is chaired by the Executive Mayor and comprises of councillors appointed by the executive mayor. |

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

| | Term | Definition |
|-------|-----------------------------|--|
| vii. | Head of Department | The head of a department of the municipality. Heads of departments are the managers referred to in section 56(a) of the Municipal Systems Act. |
| viii. | Member of Mayoral Committee | The councillor appointed by the executive mayor to be a member of the mayoral committee. |

3.4. Abbreviations

| | Abbreviation | Meaning |
|-------|---------------------|--|
| i. | HOD | Head of Department |
| ii. | CRO | Chief Risk Officer |
| iii. | CAE | Chief Audit Executive |
| iv. | SMT | Senior Management Team |
| v. | RMC | Risk Management Committee |
| vi. | CoE | City of Ekurhuleni |
| vii. | MFMA | Municipal Finance Management Act, Act No. 56 of 2003 |
| viii. | MMC | Member of Mayoral Committee |
| ix. | ERM | Enterprise Risk Management |
| x. | GRC | Governance, Risk & Compliance |
| xi. | GDS | Growth and Development Strategy |
| xii. | IDP | Integrated Development Plan (IDP |

3.5. Roles and Responsibilities

3.5.1. Council

Council is responsible for overseeing the complete spectrum of governance within the City of Ekurhuleni. This responsibility would therefore also oversight on the process of managing risks within the CoE.

3.5.2. Mayoral Committee

- (a) Mayoral Committee, chaired by the Executive Mayor, is accountable to Council and is responsible for providing political guidance, monitoring and overseeing the exercise of responsibilities assigned to the Accounting Officer for governance of risk in the CoE.

CONTROLLED DISCLOSURE

- (b) The Mayoral Committee is collectively accountable to Council in terms of the achievement of the goals and objectives of the CoE and the MMCs are individually accountable for their respective departments and entities portfolios. As risk management is an important tool to support the achievement of this goal, it is important that the members of the Mayoral Committee (MMCs) should provide political leadership, guidance and oversight to governance and risk management.
- (c) High level responsibilities of the MMCs for their respective departments and municipal entities for risk management include:
 - i. Providing oversight and direction to the department on the risk management related strategy and policies;
 - ii. Influencing how strategy and objectives are established, departmental activities are structured, and risks are identified, assessed and acted upon;

3.5.3. Audit Committee

- (a) The Audit Committee is a committee of council, comprising of independent members, responsible for assisting the Council in addressing its oversight requirements of the municipality's control, governance and risk management.
- (b) The Audit Committee's primary function is to review the effectiveness of the system of risk management ensuring that significant risk within the CoE is adequately addressed and that risks are appropriately responded to.
- (c) The Audit Committee shall further:
 - i. Review management's implementation and maintenance of and appropriate enterprise-wide risk management process.
 - ii. Provide oversight on significant risk exposures and control issues, including fraud risks and general matters of governance concern.
 - iii. Monitor the soundness of the CoE's combined risk management assurance efforts.
 - iv. Review and provide advice on the risk management processes established and maintained by management and the procedure in place to ensure that they operate as intended.

CONTROLLED DISCLOSURE

- v. The Audit Committee shall primarily fulfil its responsibilities over risk management through receipt and evaluation of reports it shall receive from the Risk Management Committee.

3.5.4. Risk Management Committee

- (a) Risk Management Committee shall be established in terms of the provision of S62(1)(c)(i) of the MFMA to advise the Accounting Officer (City Manager) in maintaining effective, efficient and transparent systems of governance, risk and compliance; and the Audit Committee in fulfilling its oversight responsibilities with respect to the governance, risk and compliance in the CoE.
- (b) The Risk Management Committee shall comprise of independent external members.
- (c) The Risk Management Committee shall:
 - i. Oversee the development and review of the ERM Policy and the ERM Framework.
 - ii. Oversee the development of any other risk management related policies and frameworks.
 - iii. Monitor implementation of the risk management policy and plan.
 - iv. Oversee that the risk management plan is widely disseminated throughout the CoE and integrated into the day-to-day activities of the CoE.
 - v. Ensure that frameworks and methodologies are implemented to increase the possibility of anticipating any risks.
 - vi. Ensure that management considers and implements appropriate risks responses.
 - vii. Ensure that continuous risk monitoring by management takes place.
 - viii. Consider and review reports from management on areas of risk, including but not limited to:
 - City-Wide Strategic risks;
 - Strategic Departmental Risks

CONTROLLED DISCLOSURE

- Operational risks;
 - Financial risks;
 - Business continuity risks;
 - Safety, health and environmental risks;
 - Loss incidents and risk financing;
 - Information and communication technology risks; and
 - Emerging risks.
- ix. Provide assurance to the Audit Committee by periodically reporting on matters it has considered.

3.5.5. City Manager

- (a) The City Manager, as accounting officer, is accountable for implementation of risk management in the CoE.
- (b) More specifically, the City Manager is responsible for:
- i. Approving the risk management framework.
 - ii. Ensuring that the risk management framework is effectively applied in the CoE and that Risk Management Office has the capacity to facilitate its application.
 - iii. Providing the authority to the Chief Risk Officer to facilitate the application of the framework throughout the CoE.
 - iv. Assigning responsibility and authority to HODs on the effective management of risks;
 - v. Providing monitoring, guidance and direction in respect of risk management;
 - vi. Ensuring that risk management performance areas, performance indicators and risk indicators are incorporated into the CoE's performance system.
 - vii. Disclosures in the annual report and various stakeholders on the effectiveness of the CoE's risk management process.

3.5.6. Chief Risk Officer

- (a) The Chief Risk Officer (CRO) has the ultimate responsibility to provide strategic direction, technical expertise, guidance, support, build capacity and to monitor departments and entities in effecting ERM.
- (b) The CRO's responsibilities include ensuring that appropriate components of ERM are in place in the CoE. The CRO generally fulfils this duty by:
- i. Setting broad-based policies and developing the CoE's ERM philosophy, risk appetite and culture for approval by the accounting officer, mayoral committee and council;

CONTROLLED DISCLOSURE

- ii. Developing and Implementing enterprise wide risk management plan which is underpinned by the organisational Growth and Development Strategy (GDS) and the Integrated Development Plan (IDP);
- iii. Developing and implementing risk management methodologies, techniques, templates and systems for gathering risk information, monitoring risk management activities, information sharing and reporting.
- iv. Providing technical advice to the accounting officer/Boards, Heads of Departments and senior management on risk management strategies;
- v. Developing and implementing initiatives and processes to inculcate an organisational culture that is aware of, appreciates and takes seriously matters of risk management;
- vi. Facilitating risk assessments and advising on the development of risk responses, as is appropriate without violating the responsibilities of risk owners
- vii. Collating, aggregating, interpreting and analysing the results of risk assessments to extract risk intelligence;
- viii. Preparing reports on risk matters for consideration by various stakeholders;

3.5.7. Governance, Risk and Compliance Forum

- (a) The Governance, Risk and Compliance (GRC) Forum is a structure established and coordinated by the Chief Risk Officer, comprising of departmental Risk Officers and Risk Champions.
- (b) The GRC Forum serves as the link between the Risk Management Department and departmental risk practitioners and assist the Senior Management Team in the performance of its responsibilities in the management of the risks in dealing with the day to day operations of the CoE.
- (c) The GRC Forum shall be utilised to:
 - i. Contribute to the development of the risk management plan.
 - ii. Communicate risk management performance expectations.
 - iii. Share knowledge on pertinent risk management matters.
 - iv. Be the platform for basic training and awareness on risk management.
 - v. Identify challenges to the implementation of risk management processes and propose solutions thereto.

CONTROLLED DISCLOSURE

3.5.8. Senior Management Team

- (a) The role of the Executive Risk Management Committee shall be assumed by the Senior Management Committee (SMT). The SMT takes strategic decisions associated with risks governance, organisation-wide risks and the response thereto in the City.
- (b) More specifically, the SMT shall be responsible for:
 - i. Reviewing and endorsing the CoE's risk management plan designed by the Chief Risk Officer;
 - ii. Inculcating a positive culture of risk management in the CoE;
 - iii. Reviewing risk management reports submitted by the Chief Risk Officer pertaining to risk;
 - iv. Considering and taking decisions on any matters and reports that have risk implications for the City
 - v. Actions to optimize risk/reward profile, maximise reward with risk contained within the approved risk appetite and tolerance limits;
 - vi. Monitoring of the ERM processes on both a detailed and macro basis by evaluating changes, or potential changes to risk profiles;
 - vii. Monitor the implementation of 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;
 - viii. Reporting to the Risk Management Committee and Audit Committee on the risk process and resultant risk/reward profiles;

3.5.9. Heads of Department

- (a) Heads of Departments (HoDs) are the owners of risks affecting their areas of accountability.
- (b) Heads of Departments are accountable to the Accounting Officer (City Manager) for designing, implementing and monitoring the process of risk management and integrating it into the day-to-day activities of their respective areas of responsibility. This is done within the context, scope and criteria for ERM as defined by the Chief Risk Officer.
- (c) More specifically, the HoDs are responsible for:
 - i. Identifying risks associated with the objectives, processes and projects within their areas of responsibility;
 - ii. Evaluating the risks identified;
 - iii. Deciding on the appropriate manner in which risks will be responded to;

CONTROLLED DISCLOSURE

- iv. Reviewing and approving the risk registers and risk management reports submitted by the Risk Champions pertaining to risk;
- v. Assigning a manager to every key risk for appropriate mitigating action and to determining an action date;
- vi. Considering the recommendations made by the internal auditors, external auditors and other assurance providers which, in their opinion, will enhance the management of risks;
- vii. Empowering officials to perform effectively in their risk management responsibilities through proper communication of responsibilities, comprehensive orientation and ongoing opportunities for skills development.
- viii. Holding officials accountable for their specific risk management responsibilities.
- ix. Maintaining a co-operative relationship with the Risk Management Department and Risk Champions
- x. As appropriate, establish departmental structures/teams to facilitate and oversee risk management processes.

3.5.10. Risk Champions

- (a) Heads of Departments shall appoint Risk Officers/Risk Champions in their respective areas of responsibility. The Risk Officers /Risk Champions assist their heads of department to:
 - i. Undertake a gap analysis of the departments ERM process at regular intervals;
 - ii. Facilitate the identification of risks of the department, as aligned to the department's priorities and objectives;
 - iii. Facilitate risk assessments;
 - iv. Facilitate the development of risk response actions
 - v. Communicates the departmental risk responses to all management levels and to employees;
 - vi. Monitor and report on the implementation of identified risk response measures;
 - vii. Compile and maintain the risk register of the Department;
 - viii. Consolidates all information pertaining to all risk related functions, processes and activities;
 - ix. Communicates with the Departmental SMT regarding the status of ERM;
 - x. Regularly interacts functional areas and meets with senior managers to promote embedding risk management into the culture and daily activities of the Department.

CONTROLLED DISCLOSURE

3.5.11. Other Officials in the CoE

- (a) Other officials are responsible for integrating risk management into their day-to-day activities. Other officials' high-level responsibilities include:
- i. Applying the risk management processes in their respective functions;
 - ii. Implementing the action plans to address the identified risks;
 - iii. Informing their supervisors and/ or the departmental risk officer/ GRC champion of new risks and significant changes in known risks; and
 - iv. Co-operating with other role-players in the risk management process and providing information as required.

3.5.12. Internal Audit

- (a) Internal Audit, headed by the Chief Audit Executive (CAE), is responsible for providing independent assurance on the effectiveness of risk management, controls and governance processes, as designed and represented by management, are adequate and function in a manner to ensure that amongst other things risks are appropriately identified and managed, based on the scope of their coverage plan.
- (b) Internal Audit shall:
- i. Provide assurance that management processes are adequate to identify and monitor significant risks;
 - ii. Use the outputs of risk assessments as one of the inputs in the development of internal audit plans;
 - iii. Provide ongoing evaluation of the risk management processes;
 - iv. Provide objective confirmations that the SMT, Risk Management Committee and Audit Committee and also provide the right quality of assurance and reliable information from management regarding risk;
 - v. Provide assurance regarding the effectiveness, efficiency and optimisation of risk responses and related control activities.

3.6. Process for Monitoring

Assurance on the implementation of the Policy will be provided by the Risk Management Committee from the reports furnished by the Chief Risk Officer.

4. Acceptance

This document has been seen and accepted by:

CONTROLLED DISCLOSURE

| Name | Designation | Capacity |
|------------------|--------------------|--|
| Phindi Shabalala | Chief Risk Officer | Head of department for Risk Management |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

5. Revisions

| Date | Rev. | Remarks |
|---------------|------|---------|
| December 2021 | 2 | N/A |

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

Annex A– Enterprise Risk Management Framework

1. INTRODUCTION

- 1.1. The City of Ekurhuleni (hereafter referred to as “CoE” or “City”) recognises that risk management and internal controls are key elements of good corporate governance and legislation. The CoE’s approach to risk management is founded upon ensuring risk is effectively and consistently managed across all levels of the municipality. The risk culture that emanates from the strategic leadership team throughout the organisation is essential in ensuring all levels buy into and adhere to the corporate risk process.
- 1.2. The City has therefore adopted an Enterprise-wide Risk Management (ERM) Framework which is designed to ensure significant risks and related incidents are identified, documented, managed, monitored and reported in a consistent and structured manner across the CoE.
- 1.3. This document provides the CoE and its employees with a comprehensive approach to identifying and managing risk in relation to this framework. It will help all employees address not only the insurable and retained risks, but also risks associated with areas such as change management, service delivery, legislative and regulatory compliance. This will provide a sound basis for corporate and operational planning, help to minimise costly surprises, lead to better outcomes in terms of program efficiency and effectiveness, as well as support management decision making on a daily basis – all of which will ultimately enhance the City’s delivery of services to the community of Ekurhuleni.
- 1.4. This document comprises two distinct components:
 - (a) An overview of the CoE’s Enterprise Risk Management Framework is provided. This maps the City’s approach and the structures and processes that support an integrated risk management environment which links business objectives, risk and related controls; and
 - (b) It sets out the specific processes associated with risk management activities within the CoE. It facilitates the preparation and documentation of comprehensive risk management plans to enable implementation of risk management practices across the CoE.
- 1.5. In addressing both the strategic, operational and process aspects of risk management in the CoE, this document is a resource available for management to use as a reference and as a basis for implementing the training required to ensure employees involved in risk management activities are appropriately skilled in the required CoE risk management processes.
- 1.6. It is expected that this document, and the methods and concepts used within it, will be reviewed, and updated periodically. Like all activities undertaken by the CoE, it will be subject to continuous improvement as new and more advanced practices in risk

CONTROLLED DISCLOSURE

management evolve. The Risk Management Framework should be read in conjunction with the Risk Management Policy of the City of Ekurhuleni.

2. PURPOSE

The purpose of the Integrated Risk Management Framework is to establish and provide for the systematic and structured processes of managing of risk.

3. OBJECTIVES OF RISK MANAGEMENT FRAMEWORK

- 3.1. Managing risk is an essential element of the City's operations. The main tools of risk management are the establishment of a coherent ERM Policy, the implementation of specific procedures with respect to operations involving certain types of risks and the placement of various authority limits on certain operations. The specific objectives of this Framework are:
- 3.1.1. To promote an awareness of risk and a responsibility for managing risk amongst all City's employees, members of public and other stakeholders who use the City's services.
 - 3.1.2. To initiate measures to reduce the City's exposure to risk and potential loss.
 - 3.1.3. To initiate measures which will enhance the City's ability to build on success and seize opportunities.
 - 3.1.4. To improve communication and sharing of risk information through all areas of the City to aid effective risk management and encourage best practice.
 - 3.1.5. To establish processes for the efficient management of risk including regular monitoring and review.
 - 3.1.6. To optimise the use of Risk Financing, Risk Mitigation and Risk Transfer mechanisms.
 - 3.1.7. To encourage a continuous and ongoing development of the process of risk understanding, review and management through the City.
 - 3.1.8. To promote open reporting of risks.

4. LEGISLATIVE MANDATE AND BEST PRACTICE

- 4.1. The City of Ekurhuleni's ERM Framework is based upon legislative requirements, good corporate governance and best practice in risk management.
- 4.2. The mandate for risk management in the City is derived primarily from Municipal Finance Management Act, 56 of 2003 (MFMA). The City of Ekurhuleni will continue to be an exemplar of good practice and to meet the City's statutory responsibility to have in place satisfactory arrangements for managing risks, as stipulated in the MFMA as follows:

Section 62 (c)(i) of the MFMA requires that:

"The accounting officer has and maintains:

CONTROLLED DISCLOSURE

(c) Effective, efficient and transparent systems of financial and risk management and internal control.

-
- 4.3. The extension of general responsibilities in terms of section 78 and 105 of the MFMA to all managers within the City implies that responsibility for risk management vests at all levels of management and that it is not limited to only the accounting officers, risk management office and internal audit.

5. BACKGROUND & CONTEXT

- 5.1. ERM forms a critical part of any institution's strategic management. It is the process whereby an institution both methodically and intuitively addresses the risk attached to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of activities. ERM is therefore recognized 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.
- 5.2. The underlying premise of risk management is that every governmental body exists to provide value for its stakeholders. Such value is based on the quality-of-service delivery to the citizens. 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 the City will manage the risks faced in its various municipal structures in an appropriate manner.
- 5.3. The City of Ekurhuleni operates in an environment 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.
- 5.4. The King IV Code of Corporate Governance emphasizes that the governing body (Council) should assume responsibility for the governance of risk by setting the direction for how risk should be approached and addressed in the organisation. Risk governance encompass both:
- the opportunities and associated risks to be considered when developing strategy; and
 - The potential positive and negative effects of the same risks on the achievement of

CONTROLLED DISCLOSURE

the City's objectives.

- 5.5. This Enterprise Risk Management Framework specifically addresses the processes and standards implemented to manage risks on an enterprise-wide basis in a consistent manner. The City and entities are obliged to adhere to the Treasury Regulations in terms of the Municipal Finance and Management Act, 2003

6. RISK MANAGEMENT CONCEPTS

6.1. Risk

- 6.1.1. King IV defines risk as follows:

“Risk is about the **uncertainty of** events, including the likelihood of such events occurring and their effect, both positive and negative, on the achievement of the organization's objectives. Risk includes uncertain events with a **potential positive effect** on the organisation (i.e. **opportunities**) not being captured or not materialising.”

- 6.1.2. The Institute of Risk Management defines **risk** as “...**the uncertainty of an event occurring that could have an impact on the achievement of objectives.**”

- 6.1.3. ISO31000 2018 defines risk as “the effect of uncertainty on objectives”.

- 6.1.4. These objectives could be strategic, operational, financial, reporting and/or compliance objectives. Some risks must be taken in pursuing opportunity, but the City should be protected against avoidable losses that could result from risks that have materialised. Risk is often characterised by reference to potential events and consequence. Risk is measured in terms of consequences of impact and likelihood.”

- 6.1.5. The management of risk is no more or less important than the management of organisational resources and opportunities and it simply forms an integral part of the process of managing those resources and opportunities.

6.2. Enterprise Risk Management

- 6.2.1. Enterprise Risk Management (ERM) deals with risks and opportunities affecting value creation or preservation and is defined as follows with reference to COSO (The Committee of Sponsoring Organizations of the Tredway Commission):

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

- 6.3. Risk Management Process

The risk management process is the systematic application of management policies procedures to the activities of establishing context, identifying, analysing, and evaluation of

CONTROLLED DISCLOSURE

actual and potential risk areas as they pertain to the City, followed by a process of, either termination, transfer, tolerance (acceptance) or treatment (reduce) through a system of appropriate internal controls. The process also includes the communicating, consulting and monitoring activities.

6.4. Risk Owner

6.4.1. A risk owner is the person/structure within the City:

- i. For whom an identified risk directly relates to their area of accountability, and is responsible for and has the authority to respond to the risk; and/or
- ii. That coordinates efforts to respond to a risk with various stakeholders who are impacted by a risk to some degree.

6.4.2. Although strictly not always the case, risk owners are typically senior managers in the City.

6.5. Key Risk Indicator

6.5.1. A Key Risk Indicator (KRI) is a measure used to indicate how risky an activity is. Key risk indicators are metrics used to indicate an increase or decrease in risk exposures for various risk categories.

6.5.2. The characteristics of a good KRI are:

- i. Ability to measure the right/relevant attributes of a risk;
- ii. Ability to be quantified;
- iii. Capability to be measured precisely and accurately;
- iv. Ability to be tracked on a regular basis by a designated risk owner;
- v. Ability to be reviewed and validated;

6.5.3. It is ideal if a KRI is aligned to a corresponding key performance indicator to facilitate tracking and measurement.

6.5.4. In the interests of practicality, and due to the variety and number of the risks that the City faces, the definition of KRIs can be performed exclusively for:

- i. Identified and prioritised areas of risk;
- ii. Certain risk categories;
- iii. Some projects
- iv. Some departments; or
- v. Some processes

6.6. Risk Appetite

6.6.1. Risk Appetite is the amount of risk the City and its MOEs is prepared to take in pursuit of value is defined as its risk appetite.

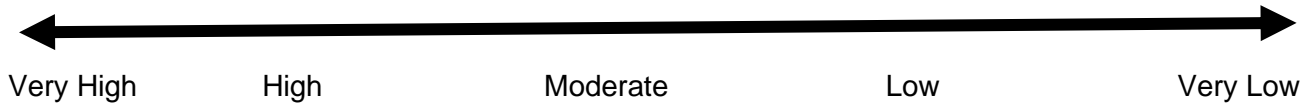
CONTROLLED DISCLOSURE

- 6.6.2. A risk appetite is articulated in the form of a risk appetite statement. A risk appetite statement is a clear, documented affirmation made by management stating its position on its tolerance or non-tolerance of certain risks.
- 6.6.3. Risk appetite can be expressed either in the form of:
- i. How much risk is tolerable, with the inference that higher risk levels will be intolerable.
 - ii. How much risk will not be tolerated, with the inference that lower levels of risk will be tolerable.
- 6.6.4. Risk appetite is the maximum exposed amount that the City is willing to accept on the basis of risk-return trade-offs for one or more desired and expected outcomes.
- 6.6.5. Risk appetite is not defined singularly for a broad range of risks. Rather, there will be a range of appetites for different types of risks which need to align. These risk appetites may also require adjustment over time.
- 6.6.6. Risk appetite statements are best aligned to a particular key risk indicator.
- 6.6.7. Risk appetite is informed by:
- i. Prescribed compliance and regulatory standards;
 - ii. The management's philosophy, values and ethics; and
 - iii. Service Delivery imperatives and targets
- 6.6.8. Risk appetites can be applied at any level of risk across the City.
- 6.6.9. The City's risk appetite can be categorized into different positions based on its posture towards risk.
- 6.6.10. These positions are shown in the diagram below:

- Aggressive attitude towards risk
- High propensity to accept or take on risk in return of high gains

- Highly averse position towards risk
- Low propensity to take on risk that has highly negative consequences and have a low likelihood of being reversed recovery

CONTROLLED DISCLOSURE



6.7. Risk Tolerance

6.7.1. Risk tolerance refers to the City's position in response to the change in the levels of risk priority before the risk appetite is reached. The tolerance for certain risk levels is dependent on the following attributes for a risk in question:

- i. Nature the risk
- ii. Risk appetite posture taken for the risk

6.7.2. The scale of risk tolerance can range from:

- i. Singular – any risk levels within the risk appetite are expressed in singular terms. For example, the levels can singularly be regarded as “medium”.
- ii. Coarse – for example, a 3 level “High, Medium, High” risk scale.
- iii. Fine – for example, a 1 to 10 scale that finely differentiates between variations in the escalating risk levels
- iv. Linear to non-linear in nature

6.8. Risk Management Capability Maturity

6.8.1. Risk management capability maturity refers to the degree to which all risk management processes in the City have been optimised to achieve the intended objectives.

6.8.2. A risk management capability maturity model is the tool that is developed to measure the levels of capability maturity for risk management.

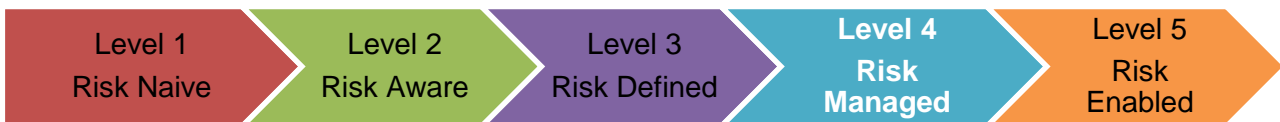
6.8.3. Risk management capability maturity is measured against the following 6 themes:

- i. Risk Management Culture - Risk culture reflects the degree to which the principles of risk management are embedded
- ii. Risk Management Strategy and Policy - Risk strategy and policy reflect the degree to which the longer-term direction and scope of risk management are established and the adequacy of the documented policy
- iii. Risk Management Structures - Risk structures are used to support risk management processes. They include the individuals and groups responsible for coordinating, managing and monitoring the risk management process
- iv. Risk Management Processes - Risk management processes are well defined to identify, assess, treat, monitor and update the risk register and risk management process integrate with other business processes

CONTROLLED DISCLOSURE

- v. Risk Management Methodology - Risk management methodology refers to the adequacy of tools, templates and techniques used to support the risk management processes including whether methodologies are consistently applied across the Organisation. It spans across risk identification, assessment, management, review and reporting
- vi. Risk Management Systems - Risk systems refer to the IT systems in place to support risk management processes and methodologies

6.8.4. Each of the following six themes is used to evaluate the extent of the City's capability maturity using the maturity level scale depicted below:



6.8.5. The attributes of each of the maturity level are defined below:

| Maturity Level | Attributes | Key Principles |
|--------------------------|---|---|
| Level 1: Risk Naïve | Dependent on heroics: Institutional capabilities lacking | <ul style="list-style-type: none"> ▪ Management have not been trained to understand what risks are, and their responsibility for them. ▪ A scoring system for assessing risk has not been defined. ▪ Management have not set up methods to monitor proper operations of key processes. |
| Level 2: Risk Aware | Process established and repeating, reliance on people continues | <ul style="list-style-type: none"> ▪ Management have been trained a little to understand what risks are, and their responsibility for them. ▪ A scoring system for assessing risk has not been defined. ▪ Risk appetite not defined. ▪ Some monitoring has been set up to monitor proper operation of key processes |
| Level 3: Risk Defined | Policies, processes and standards defined and institutionalised | <ul style="list-style-type: none"> ▪ Management have been trained to understand what risks are, and their responsibility for them. ▪ The City's objectives defined. |

CONTROLLED DISCLOSURE

| Maturity Level | Attributes | Key Principles |
|--------------------------|---|--|
| | | <ul style="list-style-type: none"> ▪ A scoring system for assessing risk has been defined. ▪ Risk Appetite defined <p>Risks are regularly reviewed Management have set up methods to monitor proper operation of key processes</p> |
| Level 4: Risk Managed | Risk measured / managed and aggregate enterprise wide | <ul style="list-style-type: none"> ▪ Management have been trained to understand what risks are, and their responsibility for them. ▪ The City's objectives defined. ▪ A scoring system for assessing risk has been defined. ▪ Risks have been collated into one list. ▪ Responses to risks have been collated. ▪ Risk appetite defined <p>Risks are regularly reviewed Management have set up methods to monitor proper operation of key processes</p> |
| Level 5: Risk Enabled | Risk management a source of competitive advantage | <ul style="list-style-type: none"> ▪ Management have been trained to understand what risks are, and their responsibility for them. ▪ All new projects are routinely assessed for risk ▪ The City's objectives defined a scoring system for assessing risk has been defined. ▪ Risks have been collated into one list. ▪ Responses to risk have been collated. ▪ Risk appetite defined Risks are regularly defined <p>Management have set up methods to monitor proper operation of key processes.</p> <ul style="list-style-type: none"> ▪ Managers provide assurance on the effectiveness of risk management |

6.8.6. The above criteria are utilised to perform risk management capability maturity assessments.

6.8.7. The frequency and timing of such assessments is decided on by management with the ultimate purpose of:

- i. Determining the prevailing capability maturity state at any point in time
- ii. Setting capability maturity targets
- iii. Facilitating and informing plans to be developed and implemented to achieve the set maturity targets.

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

7. APPROACH TO IMPLEMENTING ENTERPRISE RISK MANAGEMENT

7.1. Risk Management Approach

- 7.1.1. The City has adopted the principles of the risk management process contained in:
- i. Committee of Sponsoring Organizations of the Treadway Commission (COSO) Integrated ERM Framework.
 - ii. International Organization for Standardization. ISO 31000:2018 Risk Management Standard.
 - iii. National Treasury’s Public Sector Risk Management Framework. Both frameworks are dedicated to improving financial management, internal control and corporate governance.

7.1.2. The diagram below illustrates the basic process of risk management (as per the COSO Integrated ERM Framework), that has been adopted in this framework. The process has been adapted for the purposes of the City.



- 7.1.3. This framework defines essential components, suggests a common language, and provides clear direction and guidance for ERM.
- 7.1.4. It is important to follow this framework’s principles and/or processes when conducting risk assessments as this ensures that the City’s approach to risk management is both comprehensive and consistent.
- 7.1.5. This process is formally conducted across the entire City at least on an annual basis. This occurs in conjunction with the corporate and business planning process and involves the review and update of risk profiles for the City as a whole and includes a review for each individual business unit.
- 7.1.6. The City’s internal environment is the foundation of all other components of risk

CONTROLLED DISCLOSURE

management. It encompasses the tone of the Council and sets the basis for how risk is viewed as an enabler to the achievement of the City's goals and objectives.

7.2. Risk Management Levels

7.2.1. The City manages its risk at the following levels:

- i. **Strategic Level:** The highest level of risk is managed at this level. This level sets the tone for effective risk management across the City. At this level, the risk management plan is agreed and endorsed and its principles championed by senior management.
- ii. **Business level (Departmental) Level:** The second highest level of risk is managed at this level. This level sets the tone for effective risk management within the department. Close links between the Risk Champions and the Risk Management department strengthen the process and ensure consistency in the risk messages delivered within the services.
- iii. **Project/Programme Level:** The identification of risks from the initial business case stage in a programme/project and continued risk management throughout the project lifecycle to ensure the objectives can be achieved.
- iv. **Operational Level:** The day-to-day management processes and activities provide reasonable assurance that the main operational risks arising from service operations are identified, assessed, managed and monitored.

7.3. Relationship with other business processes

7.3.1. Risk management is not a stand-alone discipline. In order to maximise risk management benefits and opportunities, it needs to be integrated with existing business processes.

7.3.2. Some of the key business processes with which risk alignment is necessary are :

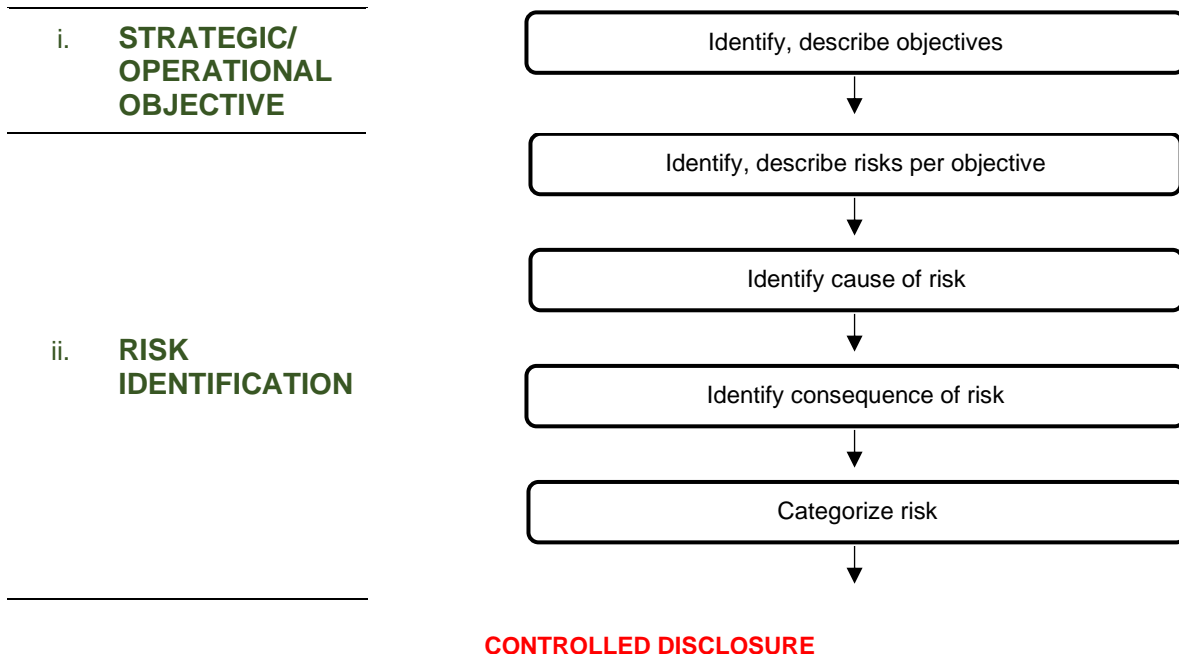
- i. **Strategic planning (including budget)** – Identifying risk during the strategic planning process allows management to set realistic delivery timelines for strategies/activities or to choose to remove a strategy/activity if the associated risks are too high or unmanageable. The impact of changing risk levels over the year can then be mapped to the relevant objective, enabling ERM to conduct more timely expectation management with key stakeholders.

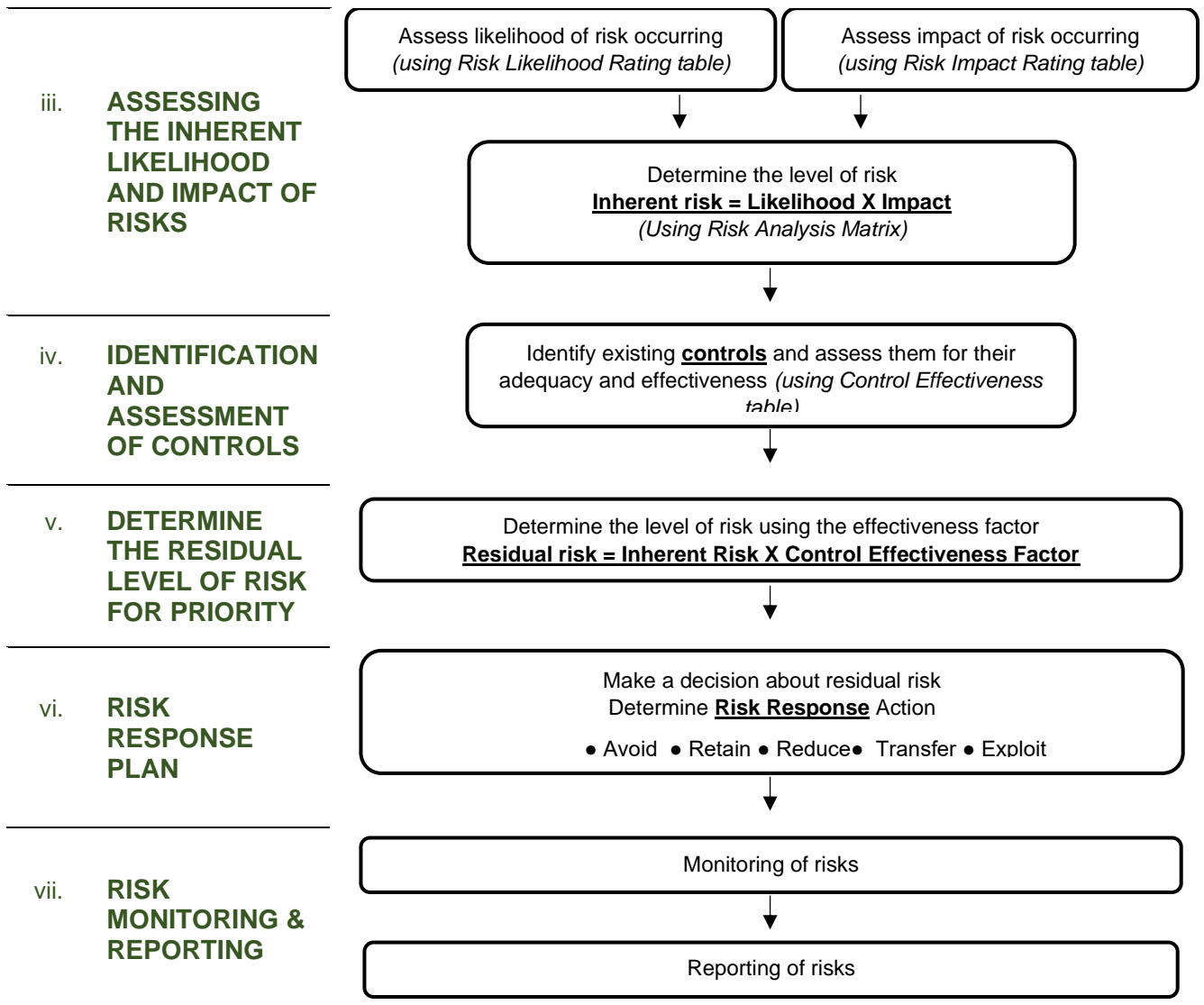
CONTROLLED DISCLOSURE

- ii. **Performance Monitoring & Evaluation** – All risk responsibilities, whether a general responsibility to use the risk management process or specific responsibilities such as risk ownership or implementation of risk treatments are included in the relevant individuals’ performance contracts and development plans.
- iii. **Internal Audit** – Internal Audit reviews the effectiveness of controls. Alignment between the internal audit function and the controls within the risk management process is critical. Internal Audit will seek to align these core processes when developing the risk based internal audit plans.

8. ENTERPRISE RISK MANAGEMENT PROCESS

- i. The risk management process is a series of logical steps which are carried out in sequence to progress through each stage of managing a risk. The process is cyclical, and it is often necessary to revisit earlier steps and carry them out again to ensure a complete picture of the risks to the activity/outcome being assessed.
- ii. A step-by-step process for risk management is depicted below with the specific steps of each sub-process thereafter:





8.1. Strategic & Operational Objectives

8.1.1. Identify and understand objectives.

8.1.2. Objectives flow from a strategic level, to a department/entity and ultimately a process level to ensure the alignment as set out below.

- i. **Strategic:** Objectives that are agreed to and approved by the Council, as contained in the IDP and the SDBIP.
- ii. **Departmental/Entity:** Objectives that are set by at Departmental or Entity level to support the achievement of the strategic objectives.
- iii. **Operational:** Objectives that are set by Management at process level to

CONTROLLED DISCLOSURE

support the departmental/entity objectives.

8.2. Risk Identification

8.2.1. Identify and understand risks

- i. Individual risk assessments will be performed to deal with the types of risks as they relate to the City as a whole, department, process or project.
- ii. One or more of the following risk identification risk identification techniques can be used:
 - (a) Facilitated risk assessment workshops;
 - (b) Discussions at management meetings;
 - (c) One-on-one interviews; and
 - (d) Analysis of financial, operational and performance data.
- iii. The above techniques could consider factors such as:
 - (a) Historical financial and non-financial performance and trends;
 - (b) Internal and external audit findings;
 - (c) Expert and specialist judgment; and
 - (d) Benchmarking risk assessments activities against other related institutions
- iv. The following will be done for each identified risk:
 - (a) A documentation of the description of the risk, actual and potential causes of the risk and consequence as well as an understanding of which objective it threatens.
 - (b) Allocation of the risk to the relevant risk category.
 - (c) Identification of a risk owner.
- v. After completion of the initial risk management process, Executive Management, in conjunction with the Risk Facilitator, will be responsible for updating the Strategic/Business/Process risk report by reassessing the status of risks and by identifying emerging risks arising through changes in the business.

8.2.2. Retirement of Risks

- i. Risks previously identified are to be retired after the circumstances that gave rise to the risk in the first place have ceased to exist. This takes place when objectives, mandates and responsibilities tied to a risk have been eliminated.
- ii. Retired risks must be classified as such and a repository of all retired risks must be maintained.
- iii. Risks that are retired shall be reported accordingly.

CONTROLLED DISCLOSURE

8.2.3. Risk Description
What can happen?

List risks, incidents or accidents that might happen by systematically working through each objective, activity or stage of your event to identify what might happen at each stage.

8.2.4. Causes of risk
How and why it can happen?

These are the causal drivers of risk that affect either the severity of impact or the likelihood of occurrence of the event or circumstance. Root Causes are typically considered as being related to Governance, People, Methods and Practices or External Factors.

In-depth consideration and in-depth analysis of risk root causes is provided below:

| | |
|---|--|
| i. Governance | Do we have the right oversight? |
| <ul style="list-style-type: none"> (a) Good governance is a fundamental part of the municipality's effective performance and an explicit part of our strategy. (b) Tone at the Top – Our values and beliefs are reflected in the way we do business. (c) Strategy and objectives – The goals of the municipality are defined, understood and implemented. (d) Policies and procedures – Our policies and procedures support our business. (e) Organisational structure – Our organisational structure supports a strong governance and effective business framework. (f) Compliance – Compliance is maintained to and enhance regulation | |
| ii. People | Do we have the right people to deliver against our goals and objectives? |
| <ul style="list-style-type: none"> (a) People across municipality are fundamental to our performance. (b) Culture – Our values and beliefs are reflected in the behaviour of our people. (c) Alignment and Co-ordination – Our people and key functions understand the link between what they do, and our strategy and objectives. (d) Competencies and Capabilities – Our people have sufficient skills and experience to meet our ongoing business requirements. (e) Roles and Responsibilities – People roles and responsibilities are aligned to our strategy and objectives. (f) Performance Measurement – The behaviour of our people is positively influenced by our measurement system. | |
| iii. Methods & Practices | Do our methods and practices support our business in the most efficient and effective way possible? |
| <ul style="list-style-type: none"> (a) Methods and practices support the municipality in efficient and effective ways of doing our business. (b) Risk Identification and Assessment – Our approach to risk management is integrated and embedded across the municipality. | |

CONTROLLED DISCLOSURE

| | |
|----------------------------------|--|
| | (c) Control Design and Effectiveness – Our controls are effectively and efficiently designed, embedded and operated across our organisation. |
| | (d) Process Improvement and Efficiency – Our programmes continually improve the ways of working to achieve maximum benefit. |
| | (e) Monitoring and Reporting – We know that our methods and practices support our goals and objectives. |
| | (f) ICT – We leverage technology effectively to support our communication and information needs. |
| iv. Environmental Factors | What is the impact of the external environment on our business? |
| | (a) The environment forms an integral part and influences the municipality's activities. |
| | (b) Political – The success of our organisation is reliant on the political support from our nation. |
| | (c) Social – Our organisation understands and aims to raise the social well-being of our people |
| | (d) Economic – The economic stability of our country is an enabler to our smooth operations. |
| | (e) Technological – The Municipality strives to improve the technological support available for better and faster operations |
| | (f) Legislative – Our organisation considers and complies with all applicable legislation |
| | (g) External stakeholders – Our external stakeholders are an integral part of all our services and we strive to provide maximum stakeholder value. |

8.2.5. Consequence

What will be the impact on objectives if they do happen?

List the possible effects of the risk should it not be managed. This is a nature and extent of consequences.

8.2.6. Risk Universe & Classification

- i. All the risks that may apply to the City's environment shall also be considered in the risk identification process. This classification of risks is known as the risk universe, and is tabled and described below:

| | RISK CATEGORY | DESCRIPTION |
|------|----------------------|---|
| i. | Economic | Risks relating to the City's economic environment such as sudden increases in unemployment and changes in the wage rates, or inflation and interest rates etc. |
| ii. | Environmental | Risks arising from the City's environment and its impact on normal operations e.g. degradation of the environment, pollution, etc. |
| iii. | Financial/Costs | Risk that the City does not have sufficient funds available to timeously fulfil its cash flow obligations. These risks could encompass non-existence of essential and |

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

| RISK CATEGORY | | DESCRIPTION |
|---------------|---------------------------------------|--|
| | | adequate financial controls, and non-compliance with relevant Treasury Regulations. |
| iv. | Fraud & Corruption | Risks relating to illegal or improper acts or conduct by employees and third parties resulting in a loss of City assets or resources. |
| v. | Governance | Failure to comply with leading practice corporate governance processes. Corporate governance is defined as a system by which City is directed and controlled. |
| vi. | Health and Safety | Risks that have a negative impact on the health and safety of the City's employees, customers, contractors and citizens arising from non-compliance with the Occupational Health and Safety Act. |
| vii. | Infrastructure | Risks emanating from the planning, development and implementation of City's infrastructural assets. |
| viii. | Legal & Compliance | <p>Risks relating to the City's legislative environment e.g. significant changes in legislation etc.</p> <p>Risks arising from violation of laws, regulations or agreements/contracts and those that may give rise to legal liability.</p> <p>Risks of potential financial loss or reputational damage caused as a result of failure to protect vested rights or obligations or abide by legal obligations and/or requirements.</p> |
| ix. | Organisational/ Business Processes | Our methods and practices to support our business in the most effective way. Methods and practices support the municipality in efficient and effective ways of doing our business. Risk of direct or indirect losses resulting from internal processes and procedures, inadequate systems or methodologies, human errors omissions, design errors, unsafe behaviour, sabotage and the actual activities undertaken by the City. |
| x. | People | <p>Risks arising from the actions or non-actions of employees, intentional or unintentional, human resource administration, and employee relations etc.</p> <p>Risk of the City failing to meet its mandate and/or objectives due to lack of critical skills capacity, loss of key executives, or retention of acquired intellectual capital.</p> <p>We have the right people to deliver. People across the municipality are fundamental to our performance.</p> |
| xi. | Political | Risk emanating from political factors and decisions that have an impact on the business mandate and operations |
| xii. | Reputation Risk | Risks that have a negative impact on the good name, public perception, image and credibility of the City. |

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

- ii. All identified risks shall be classified in terms of the categories listed in the risk universe above.
- iii. By aggregating risks horizontally across an organisation and vertically within operating departments and entities, management develops an understanding of the interrelationships between risks, gaining enhanced information as a basis for risk assessment.

8.3. Assessing Inherent Likelihood and Impact of Risks

8.3.1. Evaluating Likelihood

- i. Likelihood measures the probability that the identified risk / threat will occur within a specified period of time (between 1 and 3 years) on the basis that management have no specific / focused controls in place to address the risk/threat. The likelihood of occurrence must be assessed for every identified risk. Estimates of risk likelihood often are determined using data from past observable events, which may provide a more objective basis than entirely subjective estimates.

| CATEGORY | LIKELIHOOD OF OCCURANCE | RATING |
|----------|---|--------|
| Certain | The risk is already occurring, or is likely to occur more than once within the next 12 months | 5 |
| Likely | The risk could easily occur, and is likely to occur at least once within the next 12 months | 4 |
| Moderate | There is an above average chance that the risk will occur at least once in the next three years | 3 |
| Unlikely | The risk occurs infrequently and is unlikely to occur within the next three years | 2 |
| Rare | The risk is conceivable but is only likely to occur in extreme circumstances | 1 |

8.3.2. Evaluating Impact

- i. To assist in determining the level of impact that a risk poses for the City, the risk impact table provides a summary of each type of risk consequence relevant to the City as well as their relative severity ratings. It is also necessary to consider only the impact statements that relate to the risk being assessed, for example, a decision made by the City may have financial impact only. To ensure that all dimensions are considered, a risk in the City can have impact in terms of:
 - ii. **Strategic:** Risk impact is measured in terms of risk appetite and tolerance levels for the strategic Key Risk Indicators.
 - iii. **Departmental/Entity and Operational:** The following risk impact table is to be used to assist management in quantifying the potential impact that a risk exposure may have in terms of various types of risks.

CONTROLLED DISCLOSURE

4.4.

| Risk Impact Area | | Considerations |
|------------------|--|---|
| i. | Organisational Performance | Negative outcomes or missed opportunities that range from those that are negligible to those of critical importance to the achievement of objectives |
| ii. | Reputation | <p>The impact of the risk on the City's reputation ranges from the following states in increasing order significance:</p> <ul style="list-style-type: none"> ▪ Individual interest only, no stakeholder concerns expressed, with insignificant adverse political or reputational impact ▪ Minor stakeholder interest. Minor local media report. Minor adverse political or reputational impact. ▪ Public stakeholder discussion. Major local media interest. Moderate adverse political or reputational impact ▪ Major loss in stakeholder confidence. Significant adverse political or reputational impact. ▪ Major adverse political and reputational impact. Loss of stakeholder confidence. National media coverage. |
| iii. | Service delivery performance | <ul style="list-style-type: none"> ▪ Non-achievement of monthly service delivery targets ▪ Non-achievement of quarterly service delivery targets ▪ Non-achievement of 6-monthly service delivery targets ▪ Non-achievement of annual service delivery targets ▪ Non-achievement of mandate |
| iv. | Effect on public health, safety and property | <ul style="list-style-type: none"> ▪ Objective but reversible disability requiring medical treatment of one person. Insignificant safety impact, insignificant property damage ▪ Objective but reversible disability requiring hospitalization to several people ▪ Moderate irreversible disability or impairment to one or more people ▪ Significant irreversible injuries to up to 10 people. Single fatality ▪ Multiple fatalities and/or very serious irreversible injury to > 100 people |
| v. | Business Continuity | Interruption to services from 1 hour, ½ day, 1-5 days, 1-2 weeks to more than 3 weeks |
| vi. | Environmental Damage | <ul style="list-style-type: none"> ▪ Minor transient environmental damage, visual effects only ▪ Minor damage to environment, longer effect |

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

| Risk Impact Area | | Considerations |
|------------------|-------------------|--|
| | | <ul style="list-style-type: none"> ▪ Moderate environmental damage, local importance ▪ Major long term environmental impact. Prosecution expected ▪ Serious damage of national importance and irreversible impact. Prosecution expected. |
| vii. | Financial | <ul style="list-style-type: none"> ▪ 1% of the budget (Increase in financial costs or Loss). 1% of Revenue (revenue reduction). Insignificant issues in Auditors' Management Letter ▪ 1% <5% of the budget (Increase in financial costs or Loss). 1% <5% of Revenue (revenue reduction). Limited or no significant issues in Auditors' Management Letter ▪ 5% <10% of the budget (Increase in financial costs or Loss). 5% <10% of Revenue (revenue reduction). Issues of a serious nature are contained in the Auditors' Management Letter ▪ 10% <15% of the budget (Increase in financial costs or Loss). 10% <15% of Revenue (revenue reduction). Issues of a serious nature are contained in the Auditors' Management Letter. Qualified Audit Opinion. ▪ 15% of the budget (Increase in financial costs or Loss). 15% of Revenue (revenue reduction). Non-compliance with GAMAP/GRAP. Disclaimer or Adverse Audit Opinion |
| viii. | Projects Schedule | <ul style="list-style-type: none"> ▪ Overall schedule slips < 1% ▪ Overall schedule slips > 1% to 2% ▪ Overall schedule slips > 2% to 3% ▪ Overall schedule slips > 3 % to 5% ▪ Overall schedule slips > 5% |

8.3.3. Determining the level of inherent risk

- i. Inherent risk exposure is the risk to the organisation 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 or threats identified.
- ii. The **risk matrix** below is used to determine the level of inherent risk level or risk rating, by plotting the impact and likelihood rating and translating this information into a level of risk, from low to extreme. The risk ratings determine the nature of the risk (i.e. pre controls) and the action required to be taken by management. The level of inherent risk is calculated as Risk Impact x Risk Likelihood.

CONTROLLED DISCLOSURE

Table 3 – Inherent Risk Matrix

| | | IMPACT | | | | |
|------------|------------|----------------------|----------------------|----------------------|----------------------|----------------------|
| | | 1 Insignificant | 2 Low | 3 Moderate | 4 High | 5 Critical |
| LIKELIHOOD | 5 Certain | Insignificant (5) | Medium (10) | High (15) | Critical (20) | Critical (25) |
| | 4 Likely | Insignificant (4) | Low (8) | Medium (12) | High (16) | Critical (20) |
| | 3 Moderate | Insignificant (3) | Low (6) | Low (9) | Medium (12) | High (15) |
| | 2 Unlikely | Insignificant (2) | Insignificant (4) | Low (6) | Low (8) | Medium (10) |
| | 1 Rare | Insignificant (1) | Insignificant (2) | Insignificant (3) | Insignificant (4) | Insignificant (5) |

n of
ken.
hese
d as

8.4.2. In the City, controls generally include, but not limited to the following:

- i. Policies
- ii. Delegations & Authorisations
- iii. Operational policies
- iv. Departmental procedures and guidelines
- v. Standards or specifications
- vi. Codes of practice
- vii. Management plans, systems or structures
- viii. Regulations or other organisational protocols
- ix. Legislation.

8.4.3. The existence and proper application of these and other controls at all levels helps to ensure that the City operates efficiently, effectively and ethically.

8.4.4. 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.

| Effectiveness factor | 3.3. Qualification criteria | 3.4. 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 |

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

| | | |
|----------------|----------------------------------|------|
| Unsatisfactory | Control measures are ineffective | 0.90 |
| No control | There are no controls in place | 0.00 |

8.5. Determine the Residual Level of Risk for Priority

- i. Risk residual is the level of risk that remain after considering the impact and effect of current controls to respond to the risk.
- ii. The overall ranking of risks must be shaped by strategic and operational objectives. The ranking of risk in terms of net potential effect on strategic and operational objectives will provide management with some perspectives on priorities. This should assist in the allocation of priorities.
- iii. 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. This may be justified because non-financial influences such as operational demands, media implications, social responsibilities or regulatory pressures.

Residual risk level (magnitude) = Inherent risk level x Control effectiveness factor

| Impact | Risk acceptability | Typical Response | Rating |
|---------------|--------------------|--|--------|
| Critical | Unacceptable | Take action to reduce risk with highest priority, accounting officer/chief executive officer and Mayoral Committee/accounting authority attention. | 25 |
| High | Unacceptable | Take action to reduce risk with highest priority, accounting officer/chief executive officer and Mayoral Committee/accounting authority attention. | 20 |
| Medium | Unacceptable | Take action to reduce risk, inform senior management. | 15 |
| Low | Acceptable | No risk reduction - control, monitor, inform management. | 10 |
| Insignificant | Acceptable | No risk reduction - control, monitor, inform management. | 5 |

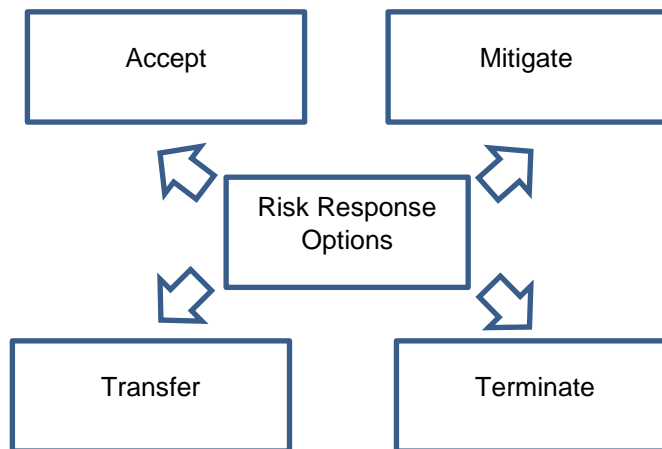
8.6. Risk Response Plan

- 8.6.1. Having assessed relevant risks, the next step is for management to determine how it will respond to these risks. Responses include risk avoidance, reduction, transfer and retention.
- 8.6.2. The gap between inherent and desired level of residual risk must result in an action. In responding to residual risk, management should assess the effect on risk likelihood and impact, as well as cost and benefits, and selecting a response that brings residual risk within desired risk tolerances.

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

8.6.3. Risk responses fall within the following categories, further described below:



| | Option | Explanation |
|-----|---------------|--|
| i | Accept Risk | <p>Management takes a conscious and deliberate decision to not directly respond to a risk because:</p> <ul style="list-style-type: none"> ▪ A temporary inability to implement risk mitigation measures ▪ High cost of mitigating a risk when compared to the benefits to be realised ▪ The factors giving rise to risk are outside of the control of the City and cannot be proactively mitigated. The City undertakes to respond to the consequences of the risk in the event that they materialise. <p>Another form of risk acceptance is the establishment of a self-insurance, in which the City will set aside financial resources in reserves that will be utilised in the event that incurs losses as a result of a type of risk materialising. Self-insurance is usually taken as a viable risk response when an assessment has been made that the City would be better off than if the Risk Transfer was taken.</p> |
| ii | Mitigate Risk | <p>Action is taken to reduce the risk likelihood or impact, or both. This may involve any of a myriad of everyday business decisions such as:</p> <ul style="list-style-type: none"> ▪ Development and revisions of operating procedures ▪ Introduction of new controls ▪ Contingency planning ▪ Revising contract conditions ▪ Disaster recovery and business continuity plan ▪ Off-site back-up ▪ Public relations initiatives ▪ Emergency procedures ▪ Staff training |
| iii | Transfer | Action is taken to reduce risk likelihood or impact by transferring or otherwise sharing |

CONTROLLED DISCLOSURE

| | Option | Explanation |
|----|----------------|---|
| | Risk | a portion of the risk. Common risk-sharing techniques include: <ul style="list-style-type: none"> ▪ Making internal financial provision for losses ▪ Purchasing insurance products ▪ Engaging in hedging transactions, or outsourcing an activity ▪ Public private partnerships and joint ventures. ▪ Taking out forward cover for foreign currency purchases. |
| iv | Terminate Risk | Action is taken to exit or not to proceed with the project, mandate or activities giving rise to risk. |

- 8.6.4. It must also be noted that multiple responses may be taken for a single risk, as deemed appropriate by management. For example, the risk of loss/damage to assets may be:
- i. Partially mitigated through the introduction of protective measure; and
 - ii. Self-Insured for losses up to a predetermined magnitude; and
 - iii. Indemnified from losses through insurance by an external financial services provider for losses in excess of self-insured loss magnitude.

8.7. Risk Monitoring and Reporting

8.7.1. Having identified the response strategy, continuous monitoring will be undertaken to ensure that the desired response for a risk is implemented successfully and achieves the desired mitigation objectives.

8.7.2. Risks will be monitored mainly through:

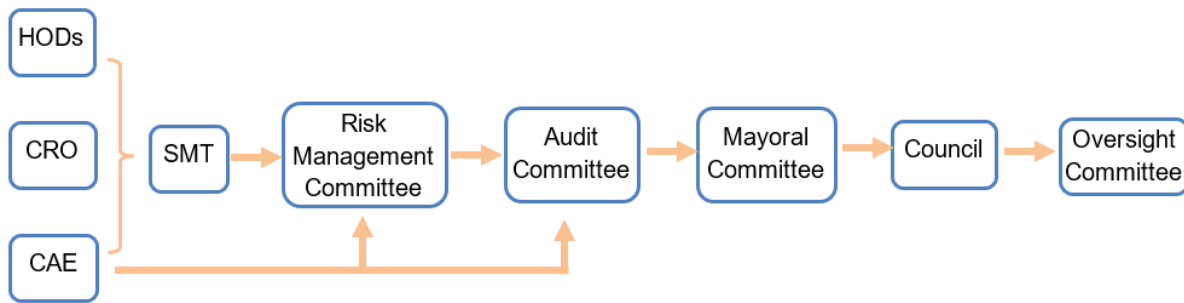
- i. The status and performance of the key risk indicators;
- ii. Whether or not the risk appetite levels have been breached;
- iii. The extent of progress of implementation of the risk action plans that are being implemented by management against the set time frames;
- iv. Any emergence of internal and external factors that have an impact of currently identified risks or give rise to new risk

8.7.3. The monitoring activities referred to above will be tracked on an on-going basis and documented once a quarter for reporting.

8.8. Risk Reporting

8.8.1. Reporting of risk information will follow the protocols as prescribed in the Enterprise Risk management Policy as follows:

CONTROLLED DISCLOSURE



- 8.8.2. The primary source of reporting on risk information is the SMT, facilitated by the Chief Risk Officer, to the Risk Management Committee.
- 8.8.3. The Risk Management Committee receives, deliberates and interrogates reports from the SMT on risks at various levels of the City as well as risks of different types.
- 8.8.4. The nature of information that is reported on risk is:
- i. Status of and any changes in the level of priority of risk
 - ii. The progress in the implementation of risk action plans
 - iii. Any actual or potential emerging risk factors that have or may have an impact on the risk landscape and control environment of the City and require escalation to higher level of authority
 - iv. Assurance information on the mitigation of risk
- 8.8.5. Risk information that requires urgent and immediate escalation may be reported at any point and in writing by any of the parties in the reporting chain described above.
- 8.8.6. The Risk Management Committee makes input and provides advice on the risk reports as presented by the management of the City and provides regular feedback to the Audit Committee.
- 8.8.7. The Risk Management Committee may also escalate any risk related matters and concerns it deems appropriate to the appropriate higher levels of accountability in the City. The response and status of risk matters escalated to any structure will be monitored for resolution.
- 8.8.8. Further reporting on risk from the Risk Management Committee will be structured and packaged in such a manner as is appropriate to further structures of municipality base on the nature of the risk information and its level of significance.

CONTROLLED DISCLOSURE

9. REFERENCES

- 9.1. The City of Ekurhuleni's ERM Framework is underpinned by legislation, South African and International Standards and a number of evolving best practice standards and guidelines.
- 9.2. The following references were used in the development of this Framework:
- i. Municipal Finance Management Act, Act No. 56 of 2003.
 - ii. Municipal Structures Act, Act No. 117 of 1998.
 - iii. Municipal Systems Act, Act No. 32 of 2000.
 - iv. King IV Report on Corporate Governance for South Africa 2016 (King IV), Institute of Directors of Southern Africa.
 - v. COSO ERM Framework 2017, Committee of Sponsoring Organisations of the Treadway Commission (COSO).
 - vi. ISO 31000:2018 Risk management – Guidelines, International Organisation for Standardisation (ISO).
 - vii. City of Ekurhuleni Risk Management Committee Terms of Reference.
 - viii. City of Ekurhuleni Risk Management Policy.
 - ix. National Treasury's Public Sector Risk Management Framework.

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.