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 (25-2022) CSSOC **CORPORATE & SHARED SERVICES OVERSIGHT COMMITTEE REPORT ON THE RISK MANAGEMENT: REQUEST FOR COUNCIL TO APPROVE THE REVISED COMPLIANCE MANAGEMENT POLICY & FRAMEWORK**

RESOLVED

1. **That** the Corporate & Shared Services Oversight Committee Report on the Risk Management: Request for council to approve the revised Compliance Management Policy & Framework **BE NOTED.**

2. **That the** Risk Management: Request for council to approve the revised Compliance Management Policy & Framework **BE APPROVED.**

3. **That** the revised Compliance Management Policy & Framework attached as **Annexure A BE RECOMMENDED** for approval

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

EKURHULENI METRO MUNICIPALITY
THE COUNCIL SECRETARY
2023 -01- 16
Signature:

SECRETARY OF COUNCIL: CITY OF EKURHULENI METROPOLITAN MUNICIPALITY

ANNEXURE A

City of Ekurhuleni	COMPLIANCE MANAGEMENT POLICY	DOCUMENT CLASIFICATION: PUBLIC

Title: **Compliance Management Policy**

Document Identifier:	
Alternative Reference Number:	
Area of Applicability:	**All CoE Departments and Entities**
Functional Area:	**All CoE Departments and Entities**
Revision:	**2**
Total Pages:	**11**
Next Review Date:	**March 2025**
Disclosure Classification:	**Controlled Disclosure**

TABLE OF CONTENTS

1. INTRODUCTION

Corporate governance, risk management and compliance (GRC) has emerged as a complex global discipline that requires effective implementation within an organisation. Such implementation enables optimal performance regular achievement of the organization's strategic goals. The City of Ekurhuleni accepts that there is a need to develop and apply sound GRC principles, including ethical values for the benefit of investors, stakeholders, and the communities within its jurisdiction.

The Municipal Finance Management Act of 2003 (MFMA) and the King IV Code on corporate governance in South Africa require a Municipality and its Entities to affect a process of ERM. The GRC function was established in the City of Ekurhuleni (CoE) to mitigate any material risk through a system of knowledge and planned controls. The City developed and implemented a GRC system that seeks to ensure that the CoE compliance risks are identified and effectively managed on a continual basis.

2. POLICY CONTENTS

2.1. POLICY STATEMENT

The City of Ekurhuleni (CoE) is committed to integrity-based performance that protects and enhances its stakeholder value and reputation. It recognises the essential role that compliance with applicable regulatory requirements plays in the governance and sustainability of its business.

The CoE subscribes to the fundamental principles that all resources will be applied economically to ensure compliance with relevant legislation, and fulfill the expectations of employees, communities, and other stakeholders in terms of corporate governance. To this end, the CoE will conduct its business in accordance with the purports and spirit of applicable regulatory requirements to ensure the implementation of appropriate processes to promote a culture of compliance within the organisation. The Municipality will do so with integrity, whilst maintaining the highest ethical standards. Although the task of designing, implementing, and monitoring the process of risk management remains the responsibility of management, the Council of CoE is ultimately accountable for the overall governance of risk and compliance. Further, Council is accountable to its stakeholders for overseeing the management of compliance within the organisation.

The management of compliance risks forms part of the overall risk management framework of the organisation. Management is responsible for ensuring that legal compliance programs are implemented and adhered to in their areas of accountability. Notwithstanding the above, the responsibility to ensure effective management of compliance risk within CoE, rests with all employees. All significant compliance risks must be assessed, managed, and reported on using a standardised methodology and a uniform compliance framework.

The Risk Management department is responsible for advising and assisting Council and Management in designing and implementing appropriate Compliance Management policies and procedures. The department creates awareness and training programs, assesses, and monitors compliance risk. It also reports on the CoE's compliance programs and practices. Further, the Department drives the implementation of strategies that reinforce a safe, transparent, and ethical working environment. The department leads the overall management and implementation of the compliance risk management process.

Our commitment to compliance risk management is an expression of our commitment to principles and good governance and alignment to best practice.
This Policy sets out CoE's approach to managing compliance risks. Further guidance and procedures can be found in the Compliance Framework.

2.2. POLICY PRINCIPLES

All staff members should take into account the following key principles, which should be adhered to in the implementation of business activities:

2.2.1. Adhering to Laws, Regulations, Policies and Procedures
2.2.2. Structured processes in place to ensure Compliance
2.2.3. Communication and Training
2.2.4. Respond effectively to instances of Non-Compliance

3. PURPOSE

The purpose of this policy is to:

3.1. Encourage the efficient use of resources towards better service delivery.
3.2. Improve accountability for the stewardship of those resources.
3.3. Align as close as possible the interests of individuals, Council, departments, and society as a whole.
3.4. Dismantle the notion of municipal inefficiencies exacerbated by previous legacies.
3.5. Enable decision makers to select best possible options to achieve objectives.

4.POLICY PROVISIONS

4.1. MANDATE OF COMPLIANCE FUNCTION

The King IV Code on Corporate Governance recommends that the Board/Council of CoE should assume responsibility for the governance of compliance with applicable laws. It encourages the adoption of non-binding rules, codes and standards when defining a compliance program.

The Council of CoE shall approve a policy that articulates and gives effect to its compliance methodology. The policy must concisely define the non-binding rules, codes and standards that are applicable.

4.2. GOVERNANCE STRUCTURE

CoE has established an independent Compliance Function, headed by the HoD Risk Management within the Risk Management Department. It is responsible for the management of the Compliance Risk within CoE and its Entities. It primarily carries out its mandate by ensuring that standardised risk based compliance processes are applied consistently in all departments. This provides reasonable assurance that CoE complies with all applicable laws and regulations. Further, it seeks to ensure that the risk of non-compliance with applicable laws is minimal across the Municipality.

The compliance function shall be managed by a Divisional Head: Governance and Compliance within the Risk Management Department. Further support will be from relevant Departmental resources who shall be responsible for facilitating and implementing the compliance processes, and systems within their departments and reporting into the risk management department and the Risk Management Committee (RMC). Refer to **Annexure A** for the **Oversight Risk Governance Structure.**

5. SUPPORTING CLAUSES

Additional policies may be developed in support of the aims and objectives of this policy, and are seen as equal in stature. Provisions of this document will apply to all policies developed in terms of this clause, except where specifically stated.

5.1. SCOPE OF APPLICATION

This policy shall apply throughout the City of Ekurhuleni's entities.

5.2. INFORMATIVE REFERENCES

Description	Context and relevance
Municipal Finance Management Act, no 56 of 2003	Details the financial arrangements prescribed for Municipalities
Municipal Systems Act	Legal authority of Municipality to regulate their operations through policies
Companies Act, 73 of 2008	To ensure that the Governance structures within the Entity are aligned with the Companies Act
KING IV Report on Corporate Governance	To align the CoE entities with industry best practice

5.3. DEFINITIONS AND ACRONYMS

Term	Description
"CoE"	*means the City of Ekurhuleni*
"Employee"	*means a person in the employ of the CoE or an Entity of the CoE*
"Councillor"	*means active Councillor of the CoE*
"Council"	*means the legally constituted Council of the CoE.*
"Structures Act"	*means the Municipal Structures* Act, Act 117 of 1998 and the regulations promulgated in terms thereof.
"Systems Act"	means the Local Government: Municipal Systems Act, Act 32 of 2000 and the regulations promulgated in terms thereof.
IDP	*Means Integrated Development Plan*
ICT	*Means the Information, Communication and Technology department*
CEO	*Means the Chief Executive Officer of an Entity; may be referred to as the Managing Director. The title refers to anyone who is the Accounting Officer*

5.4. CONTEXTUAL FUNCTIONS

5.4.1. Compliance Function: Risk Management Department

The compliance function has the ultimate responsibility to provide direction, technical expertise, guidance, support, build capacity and to monitor Departments and Entities in implementing the compliance management process.

The primary role of the compliance function is to assist with, enable, facilitate and monitor the effective management of the compliance risk of the municipality through inter alia, the following:

i. Ensuring that the compliance strategy is aligned to the enterprise-wide risk management strategy and framework which is underpinned by the organisational Growth and Development Strategy (GDS) and the Integrated Development Plan (IDP);
ii. Developing and implementing the compliance framework and; Developing and implementing the integrity and ethics framework;
iii. Ensuring that standard risk based regulatory compliance processes, including processes to identify the relevant regulatory frameworks; controls and systems are based on international compliance best practice.
iv. Developing and reviewing the Compliance policy, framework and, processes.
v. Implement and managing the standard risk-based compliance processes, controls and systems across CoE.
vi. Developing and implementing compliance management methodologies, techniques, templates and systems for gathering risk information, monitoring compliance management activities, information sharing and reporting.

vii. Providing technical advice to the accounting officer/boards, heads of departments and senior management on compliance risk management strategies;
viii. Developing and facilitating compliance risk management training and awareness programs at appropriate levels within the CoE to inculcate a compliance culture;
ix. Ensuring that the Heads of Departments and Senior Management are trained in the application of the various elements of the group compliance process and in the various roles and responsibilities.
x. Consolidating the CoE compliance risk profile and escalate critical risks to the Strategic Management Team (SMT EXCO), CoE Risk Management Committee, Audit Committee and Mayoral Committee;
xi. Reviewing reports of non-compliance incidents and major frauds and corruption (both potential and actual) including the evaluation of the effectiveness of the response in investigating any loss and preventing future occurrences;
xii. Assisting departments and municipal owned entities in facilitating compliance risk assessments and developing compliance risk mitigation strategies;
xiii. Benchmarking the performance of the risk management process to the risk management processes adopted by other municipalities both within South Africa and abroad; and
xiv. Reviewing all compliance reports prior to approval and submission to the relevant stakeholders.
xv. Developing and monitoring the implementation of the compliance framework.
xvi. Ensuring that designated CoE employees undergo compliance training and receive on-going awareness training regarding compliance to legal requirements, compliance policies and procedures.

5.4.2. CoE Compliance Function: Corporate Legal Department

i. Identification of the regulatory universe applicable to the CoE and ensuring that it is updated periodically and communicated.
ii. Conduct or arrange information sessions or workshops to educate on legal compliance requirements and changes to important legislation.
iii. Provide advice on legal compliance to departments and committees.
iv. Consider and advise on any matter that has legal, legal compliance and litigation consequences to the Municipality – including but not limited to matters referred through PAJA, Consumer Protection Act, Public Protector Act, PAIA and POPI; and provide responses on behalf of the Municipality or the Information Officer (as the case may be);
v. Compiling PAIA/POPI Manual and coordinate annual statistics and reporting to the Information Regulator and/or any other chapter nine Constitutional Institutions where required.
vi. Design framework and standards for By-law promulgation and enforcement.
vii. Enhance legal awareness and legal information/research resources in the organisation through inter alia the provision on Intranet of an electronic legal library and the provision of legal compliance registers such as the approved Municipal Code, System of Delegations, Register of Tariffs and Policies and provide legal interpretation
viii. Provide a Legal library as an information/research desk available throughout the organisation linked to the Knowledge Management Centre.
ix. Legal updates - Scrutinize Gazettes for new legislation, notices, etc. and ensuring that all relevant departments and stakeholders are informed.

5.4.3. CoE Departmental Compliance Functions:

i. Ensure effective implementation of the standard risk-based compliance processes, controls and systems for each respective CoE department.
ii. Ensure that compliance risk assessments are held annually to review and/or update the regulatory universe applicable and to assess and prioritise compliance risk.
iii. Ensure that compliance processes and controls relating to material compliance risks are documented in a systematic and standard manner.
iv. Ensure consistent monitoring and reporting on all compliance risks, assessing that the control environment is adequate and effective.
v. Ensure that the adequacy of compliance processes and the outcomes of such processes are systematically reported against, in a standardised manner to the appropriate management and governance forums.
vi. Establishing and maintaining a compliance culture, in conjunction with management, which contributes to the overall objective of prudent risk management of the municipality.
vii. Setting a tone at the top in the department that is supportive of the effective implementation of all the elements of the general compliance process and compliance programs.
viii. Ensuring that the appropriate staff members are involved and engaged in the application of the various elements of the general compliance process and in implementing compliance programs.
ix. Ensuring the ongoing monitoring of the implementation of the general compliance process, mitigating steps (i.e., the detailed implementation of compliance programs in the department) and reporting to appropriate governance structures.

5.4.4. Compliance function: Independence

i. The Compliance Officer must at all times maintain a high degree of professional independence.
ii. The diagram set out in Annexure A; serves to highlight key aspects of reporting lines that will enhance independence.

5.4.4.1. Aspects of independence:

i. In the final analysis, independence is a state of mind. In achieving this state of mind, the compliance officer should not only be independent but rather they should also be seen to be independent.
ii. The compliance officer should not have any conflict of interest that would impair their independence.
iii. Independence is central to the success of the compliance function. Without an adequate level of independence, a compliance officer would be faced with significant and perhaps insurmountable challenges.

5.5. ROLES AND RESPONSIBILITIES

5.5.1 The Mayoral Committee 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 compliance risk in the CoE.

5.5.2 The Accounting Officer (City Manager) of the CoE and the Boards of each Municipal Entity are ultimately responsible for implementation of the compliance framework in the CoE.

5.5.3 All Heads of Departments (HODs) and Chief Executive Officers (CEOs) are responsible for implementing the compliance framework in their respective Departments and municipal entities.

5.5.4 Divisional Heads/Delegated GRC functions support the compliance framework, risk management philosophy, promote compliance within our risk appetite and manage compliance risks within their spheres of responsibility consistent with set risk tolerances.

5.5.5 All employees of the CoE are responsible for implementing the compliance framework in accordance with established directives and protocols.

5.6. COMPLIANCE RISK

Compliance is the process that records and monitors the daily business activities of an organisation to make sure that it is complying with the law, industry mandates, and internal policies.

Compliance risk is the threat posed to an organisation's earnings, capital or reputation as a result of violation or non-conformance with laws, regulations, or prescribed practices. Organisations that fail to comply with the necessary standards may be subjected to fines, payment of damages, and voided contracts. This, in turn, can lead to diminished reputation and limited business opportunities as the organisation faces decreased stakeholder trust. Illegal conduct may prejudice the City of Ekurhuleni in many ways. The mere hint of illegal conduct may alter public opinion and adversely affect the behaviour of our community, customers, suppliers, business partners or shareholders.

5.7. REPORTING NON-COMPLIANCE

All instances of non-compliance shall be reported, and employees have the option to report such noncompliance or potential non-compliance to the Risk Management Department or by way of the anonymous independent ethics hotline reporting mechanism. It is CoE's policy to independently investigate all instances of non-compliance and to take the appropriate steps to mitigate the consequences of non-compliance

5.8. REMEDIAL ACTION

Any breach of this Compliance Policy and Framework is considered serious and remedial action will result in disciplinary action that could lead to dismissal.

6. ACCEPTANCE

This document has been seen and accepted by:

Name	Designation	Capacity
Risk Management Department	Governance and Compliance Management	Drafter of the policy
Governance Risk and Compliance Forum	Departmental Governance Risk and Compliance practitioners	Departmental GRC representatives
Senior Management Team (SMT)	Heads Of Departments	Policy custodians
Corporate Legal Services	DH: Corporate Legal Services	Vetting
Risk Management Committee (RMC)	Risk Management Committee	Recommend to Council for approval

7. REVISIONS

The review of this policy may be conducted annually or once in every Three (3) years, depending on the nature of the need to review. A policy may also be reviewed as and when the need to do so arises. This may depend on a change in circumstances, such as the law or national policy on the matter or issue.

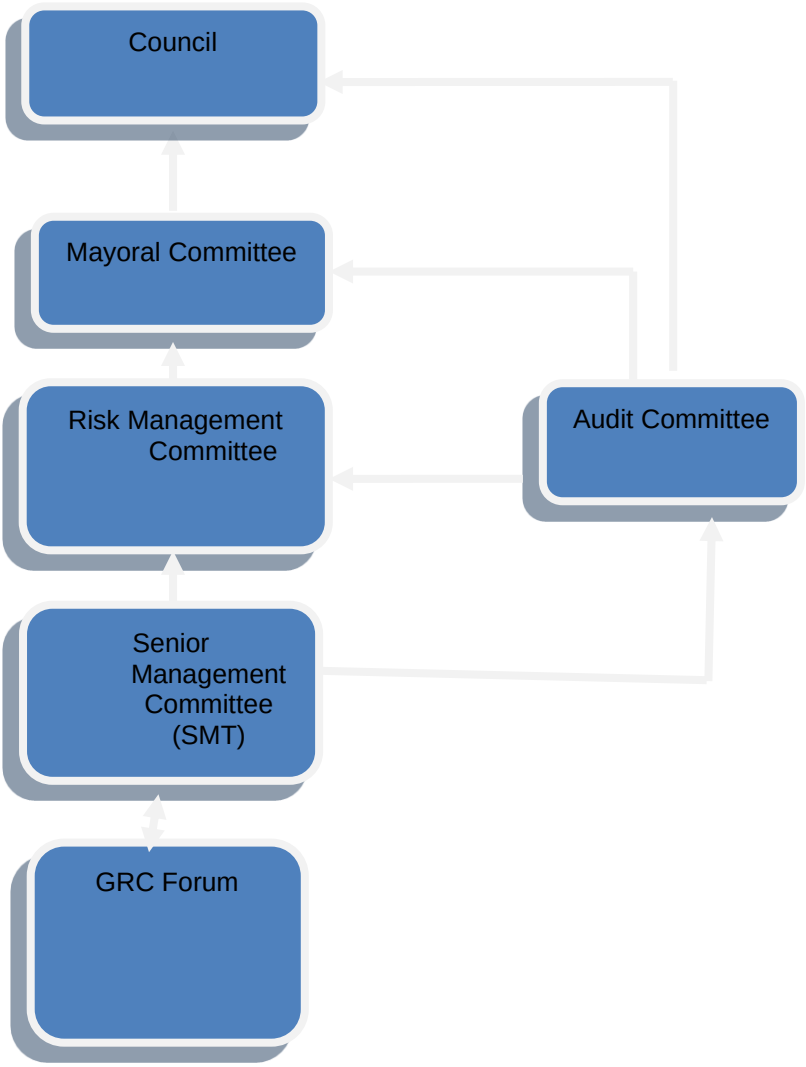
Date	Rev.	Remarks
August 2025	2	The policies of the CoE are generally reviewed on 3yr intervals or as and when required due to changes in Legislation or when necessary for operational reasons.
2015/2016 Financial year	1	The first Compliance policy was approved by Council in 2017.

8. APPROVAL

8.1. This Compliance Management Policy may only be approved by Council of the CoE.

9. ANNEXURE/S

9.1. ANNEXURE A: OVERSIGHT COMPLIANCE RISK GOVERNANCE STRUCTURES



Title: **CoE's COMPLIANCE FRAMEWORK**

Document Identifier: Version 1.

Alternative Reference Number:

Area of Applicability: All CoE Departments and Entities

Functional Area: All CoE Departments and Entities

Revision:	**1**
Total Pages:	**21**
Next Review Date:	**03/2025**
Disclosure Classification:	**Controlled Disclosure**

TABLE OF CONTENTS

1. INTRODUCTION

The establishment of the City of Ekurhuleni's (CoE) Compliance Function ("Compliance Function") originated from the need for a structured and formalised Compliance program. This function would focus on the management of compliance risks as part of a broader risk management framework. The Compliance Function is further entrenched by a King IV principle, which recommends that the Council and City Manager of CoE should ensure that CoE complies with applicable regulatory requirements.

1.1. Compliance risk is the current and prospective risk of damage to CoE's business model, business objectives, financial soundness, and reputation, arising from non-adherence to applicable regulatory requirements. Compliance risk consists of two elements, namely:

1.1.1. Regulatory element: The risk that CoE does not comply with applicable regulatory requirements or the exclusion of applicable regulatory requirements from operational business processes and procedures; and
1.1.2. Reputational element: The risk that CoE is exposed to negative publicity due to inter alia the contravention of applicable regulatory requirements during the conducting of its business.

1.2. The reasons for the existence of an independent Compliance Function are as follows:

1.2.1. To assist with ensuring compliance with applicable regulatory requirements.
1.2.2. To effectively manage and mitigate compliance risks within the broader risk management framework
1.2.3. To align with national and international compliance developments/trends/best practice.
1.2.4. To facilitate the establishment and enhancement of a compliance culture within CoE.
1.2.5. To provide for formal and structured monitoring of compliance risks in order to provide independent assurance to the Council, City Manager and Management.

1.3. The existence of the Compliance Function holds, inter alia, the following benefits for CoE:

1.3.1. To lower the impact of regulatory risk due to the continuous focus placed on compliance with applicable regulatory requirements.
1.3.2. To lower the impact of reputational risk due to the continuous focus placed on maintaining high standards of integrity at all levels, fair dealings with stakeholders (regulators, shareholders, and clients), the provision of a service based on quality and competence; and
1.3.3. To lower the impact of possible monetary operational loss due to the continuous focus placed on compliance with applicable regulatory requirements, through a culture of compliance.

1.4. Non-management of compliance risks could ultimately lead to one or more of the following:

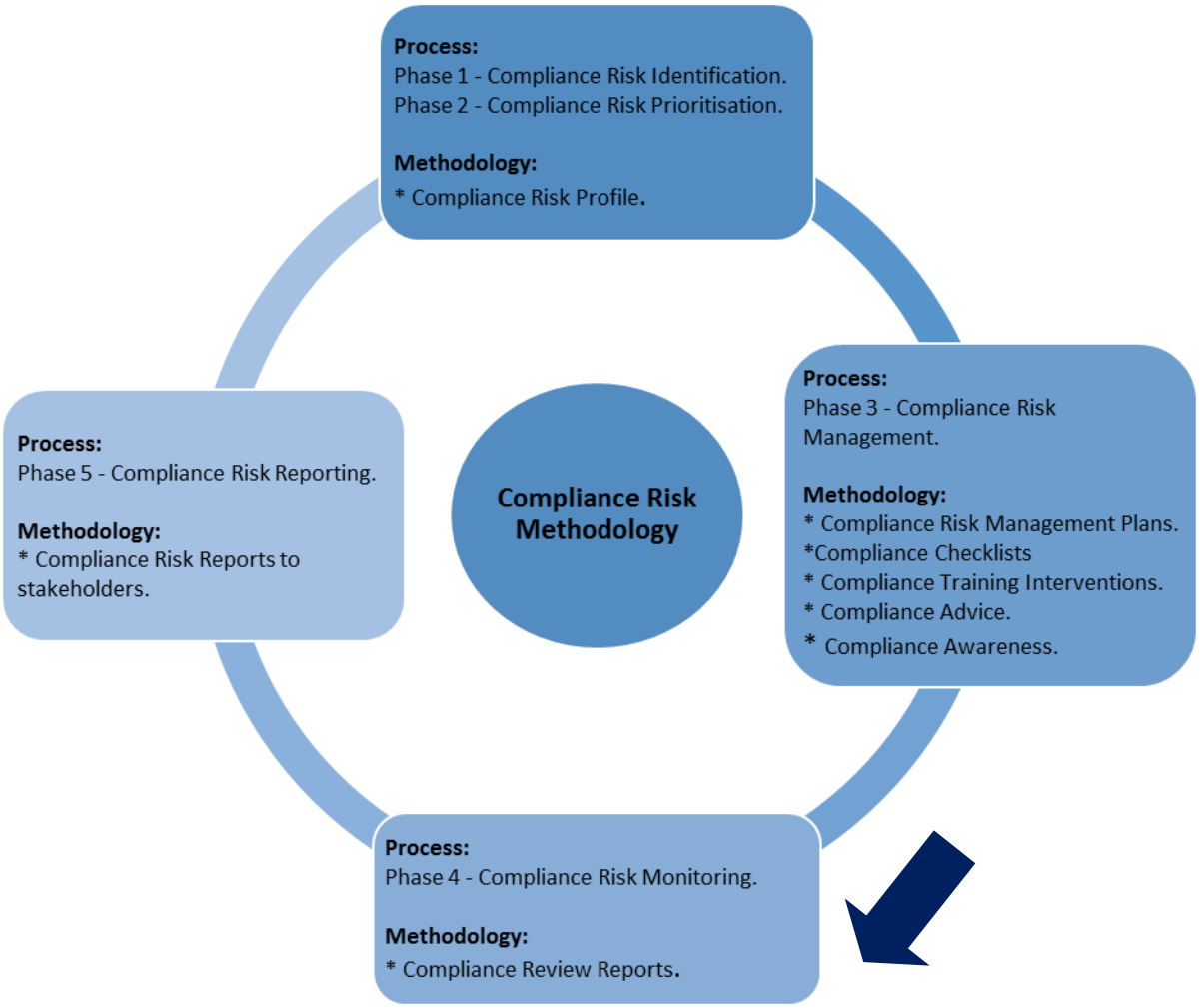
1.4.1. Fines/penalties.
1.4.2. Operational financial loss.
1.4.3. Civil/criminal charges and claims.
1.4.4. Public reprimands and associated reputational damage; and
1.4.5. Imprisonment.

2. FRAMEWORK CONTENTS

2.1. COMPLIANCE RISK METHODOLOGY

The economical and efficient management of the compliance risks that CoE is exposed to is dependent on the development and implementation of a group-wide risk-based process to manage and mitigate the compliance risks applicable to each department. The Compliance Risk Methodology provides for a visible, formalised, and structured risk-based procedure to manage and reduce the compliance risks to a level acceptable to CoE. Optimal collaboration between Governance and Compliance practitioners for each department and the Compliance Function is imperative to ensure the Compliance Risk Methodology is applied in a uniform and consistent manner.

Below is a graphical illustration of the Compliance Risk Methodology which consists of 5 phases, each phase is discussed in detail below:



2.1. Phase 1: Compliance Risk Identification/Phase 2: Compliance Risk Assessment

2.1.1. Phase 1: Compliance Risk Identification

Compliance Risk Identification involves the identification of all legislation applicable to CoE as a whole and per department – this is known as the Regulatory Universe. Ascertaining the regulatory landscape applicable to each department is essential in order to assess all applicable risks effectively.

An annual workshop is conducted and facilitated by the DH: Governance and Compliance and will include key role players. The department head or his/her nominee is requested to select the participants to the workshop, thereby ensuring that the correct participants are involved in the workshop and that the Compliance Risk Profile is accurate and supported. The participants should ideally consist of a combination of management (Executive/Middle Management) and operational staff. Workshop material is distributed to the workshop participants prior to the workshop to enable them to prepare for the workshop. Pre-workshop engagements are encouraged to discuss issues of concern and clarify matters.

The workshop participants confirm the regulatory requirements applicable to the department on a control self-assessment basis, utilising the CoE Regulatory Universe. The Compliance Risk Profile Workshop is utilised to note down the applicable regulatory requirements. Further the discussion guides the Governance & Compliance division when designing and/or procuring Compliance checklists. These checklists are focussed per piece of Legislation that has been deemed High Risk for a specific department.

2.1.2. Phase 2: Compliance Risk Assessment

Compliance Risk Assessment involves the prioritisation of the applicable regulatory requirements by rating each regulatory requirement individually. The workshop participants assess the regulatory requirements applicable to the department on a control self-assessment basis, utilising the Compliance Risk Impact/Probability Rating Scale. The Compliance Risk Profile is utilised to note down the prioritisation of each regulatory requirement.

After the workshop, the **Compliance Risk Profile** is completed, which will visually highlight the compliance risks that each CoE department is exposed to in order for CoE to prioritise its risk management strategies accordingly. Further a focussed checklist is then designed to ascertain the level of departmental compliance based on the final Compliance Risk Profile. This exercise will also assist with understanding and reporting on CoE's compliance risks as a whole.

The regulatory requirements are prioritised by individually measuring the impact and probability of each regulatory requirement:

Step 1: Rate Likelihood/Probability:

Probability is an indication of the likelihood that non-compliance with a specific regulatory requirement may occur, after having considered the control measures that have been implemented to manage and mitigate the risk. The following critical control measures are considered when measuring probability:

Likelihood category	Category definition	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

A new regulatory requirement implies greater probability; a complex regulatory requirement implies greater probability; incomplete and inaccurate information implies greater probability; etc.

Step 2: Rate Impact (also known as Seriousness):

Impact is an indication of the negative effect that non-compliance with a specific regulatory requirement can have on the department and/or COE. When measuring impact, the inherent risk (worst-case scenario) is determined, i.e., the level of risk prior to considering the control measures implemented to manage and mitigate the risk.

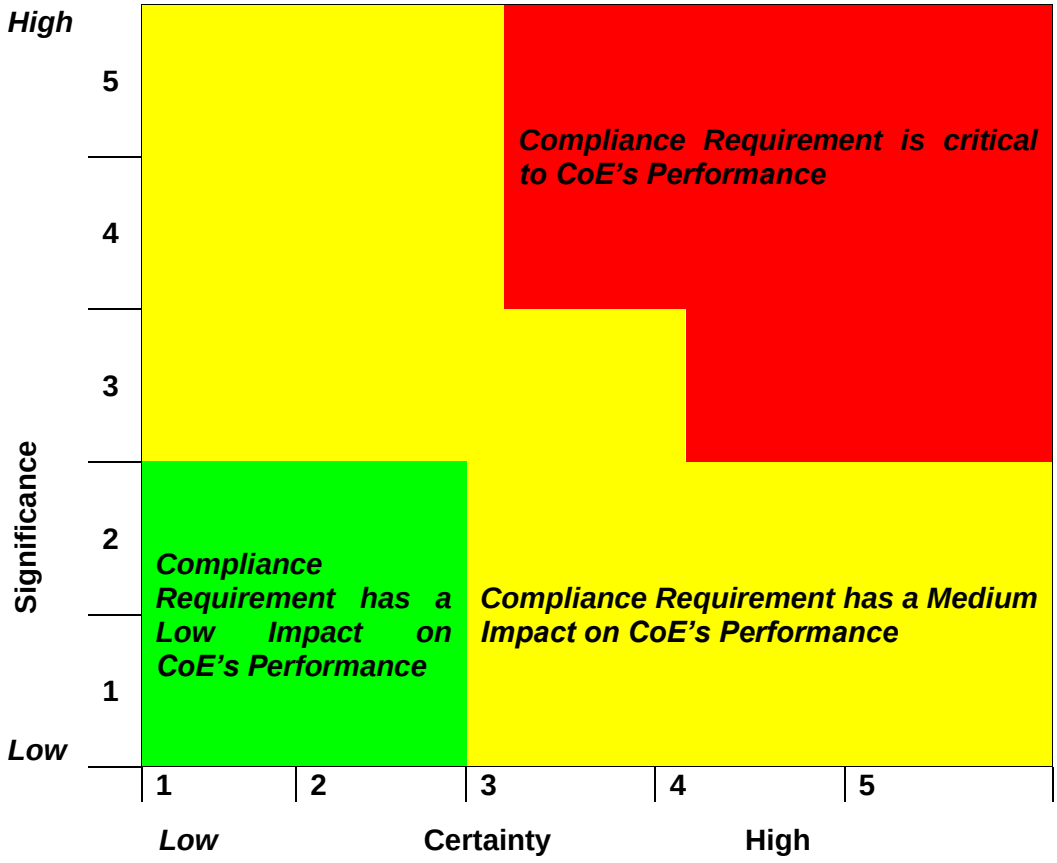
The following table is to be used to assist management in quantifying the potential impact that a risk exposure may have on the institution.

Risk Rating	Reputation	Effect on public health, safety and property	Environmental Damage	Financial	Compliance
1. Insignificant	Individual interest only, no stakeholder concern Insignificant adverse political or reputational impact	Objective but reversible disability requiring medical treatment of one person. insignificant safety impact, insignificant property damage	Minor transient environmental damage, visual effects only	1% of the budget (Increase in financial costs or Loss) 1% of Revenue (revenue reduction) insignificant issues in Auditors' Management Letter	Minor legal issues or non-compliance with regulation
2. Low	Minor stakeholder interest, minor local media report Minor adverse political or reputational impact	Objective but reversible disability requiring hospitalisation to several people	Minor damage to environment, longer effect	≥ 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	Breach of regulations/legislation with minor fines
3. Moderate	Public stakeholder discussion,	Moderate irreversible disability or impairment to one or more	Moderate environmental damage, local importance	≥ 5% <10% of the budget (Increase in financial costs or Loss)	Major breach of regulation with significant fine Significant litigation

Risk Rating	Reputation	Effect on public health, safety and property	Environmental Damage	Financial	Compliance
	major local media interest Moderate adverse political or reputational impact	people		≥ 5% <10% of Revenue (revenue reduction) Issues of a serious nature are contained in the Auditors' Management Letter	involving many weeks of management time
4. High	Major loss in stakeholder confidence Significant adverse political or reputational impact	Significant irreversible injuries to up to 10 people single fatality	Major long term environmental impact. Prosecution expected	≥ 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	Major litigation or damages prosecution with damages of R50M+ plus significant costs Custodial sentence for the municipalities Executive Directors Investigation by the Department of local government Municipality placed under administration
5. Critical	Major adverse political and reputational impact Loss of stakeholder confidence National media	Multiple fatalities and or Very serious irreversible injury to > 100 people	Serious damage of national importance and irreversible impact. Prosecution expected.	≥ 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	Major litigation or damages prosecution with damages of R100M+ plus significant costs Custodial sentence for the municipalities Accounting Officer Municipality placed under administration

Risk Rating	Reputation	Effect on public health, safety and property	Environmental Damage	Financial	Compliance

Step 3: Prioritisation:
The overall impact and probability ratings of a regulatory requirement serve as indicators to prioritise the level of risk of the regulatory requirement, between 1 and 5, utilising the following table to determine the risk level:



Inherent Risk Exposure

Inherent risk exposure is the risk to the organisation in the absence of interventions management might take to alter either the impact or likelihood of a risk. 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 table below is to be used to assist management in quantifying the inherent risk of a particular risk (i.e., pre controls)

Inherent risk exposure	**Factor**
Critical	**20.1< 25**
High	**≥ 15 <20**
Medium	**≥ 10 < 15**
Low	**≥ 5 < 10**
Insignificant	**5**

Step 4: Evaluating Effect of Response on Residual and Desired Residual Risk

Each risk is rated according to the inherent risk rating criteria. The effectiveness of the existing risk responses is then assessed. This is done by rating the control effectiveness after which it is ascertained whether or not the risk is managed to the desired level within the CoE's risk appetite. This process is an assessment of current residual risk.

The residual rating can then be ascertained by assessing the probability of a non-compliance occurring and controls that are currently in place considering the following:

i. Technology Control Measure:

Technology Control Measure refers to the extent to which current existing systems ensure compliance with applicable regulatory requirements.

ii. Information Control Measure:

Information Control Measure refers to the extent to which current available information informs employees of the provisions of applicable regulatory requirements and its implications to the Department and/or CoE; including the extent to which awareness in respect of the available information has been created and is being maintained.

iii. Policies, Processes and Procedures Control Measure:

Policies, Processes and Procedures Control Measure refer to the extent to which current existing policies, processes and procedures ensure compliance with applicable regulatory requirements.

iv. People Control Measure:

People Control Measure refers to the extent to which employees that are responsible for implementing the systems, policies, processes, and procedures; are properly trained and adequately skilled to ensure compliance with the applicable regulatory requirements.
Residual risk is calculated by multiplying the inherent risk score by the rating scale for control effectiveness.

Rating	**Effectiveness**	**Category definition**	**Factor**

	category		
1	Very good	Risk exposure is effectively controlled and managed	0.20
2	Good	Majority of risk exposure is effectively controlled and managed	0.40
3	Satisfactory	There is room for some improvement	0.65
4	Weak	Some of the risk exposure appears to be controlled, but there are major deficiencies	0.80
5	Unsatisfactory	Control measures are ineffective	0.90

The Compliance Function follows a risk-based approach in that the regulatory requirements prioritised as a Level 4 or Level 5 risk are afforded first priority in the management of the compliance risks subject to resource availability and capacity. CoE must however always comply with all applicable regulatory requirements.

The identified and assessed regulatory requirements are referred to as the department's Compliance Risk Profile. A Compliance Risk Profile Report is issued to the Head of Department and to the Compliance Function. The Compliance Risk Profile is an essential initial step in the implementation of an efficient Compliance Risk Management Framework as it highlights the compliance risks that the department is exposed to in order for the department to prioritise its risk management strategies accordingly.

2.1.3. Phase 3 – Compliance Risk Management

On completion of the Compliance Risk Identification (Phase 1) and Compliance Risk Assessment (Phase 2), Compliance Risk Management (Phase 3) commences. Compliance Risk Management (Phase 3) consists of:

a) Compliance Risk Management Plans
b) Compliance Awareness
c) Compliance Checklists
d) Compliance Training
e) Policy development in relation to specific legislation
f) Standard operating procedures

2.1.3.1. Compliance Risk Management Plans

Compliance Risk Management Plans are compiled for high risks and serve as a tracking tool for management. CRMPs give an overview on the current status of the department's regulatory control environment. Dependent on the scope and complexity of the department's Compliance Risk Profile, an individual Compliance Risk Management Plan can be developed per regulatory requirement, or a consolidated Compliance Risk Management Plan can be developed that includes more than one regulatory requirement. The Compliance function together with the relevant Divisional Head facilitates the compilation of the Compliance Risk Management Plans for the department. The department is responsible for implementing the controls and for ensuring that the controls remain adequate and effective. The Compliance Risk Management Plans are updated on an annual basis to ensure that it remains current and an active management tool.

The Compliance Risk Management Plan contains, as a minimum, the following information:

2.1.3.2. Regulatory Requirement Provisions:

The applicable provisions (provisions that have a specific compliance obligation, and which need a response in the form of a control) are recorded in the Compliance Risk Management Plan. The provisions that are not applicable should either not be recorded in the Compliance Risk Management Plan or if recorded the provisions must be indicated as 'Not Applicable'.

2.1.3.3. Controls:

The controls that address the risk of non-compliance with the applicable provisions are recorded in the Compliance Risk Management Plan. A guideline to the formulation of a good control is to ask and answer the questions:

i. What (must be done to minimise the risk?)
ii. When (must it be done?)
iii. How (must it be done?)

The critical control measures considered when recording the controls are:

2.1.3.4. Technology Control Measure:

Technology Control Measure refers to the extent to which current existing technology systems ensure compliance with applicable regulatory requirements.

2.1.3.5. Information Control Measure:

Information Control Measure refers to the extent to which current available information informs employees of the provisions of applicable regulatory requirements and its implications to the department and/or EMM and the extent to which awareness in respect of the available information has been created and is being maintained.

2.1.3.6. Policies, Processes and Procedures Control Measure:

Policies, Processes and Procedures Control Measure refer to the extent to which current existing policies, processes and procedures ensure compliance with applicable regulatory requirements.

2.1.3.7. People Control Measure:

People Control Measure refers to the extent to which employees, responsible for implementing the technology systems; and the policies, processes and procedures; are properly trained and adequately skilled to ensure compliance with the applicable regulatory requirements.

Three types of controls are regarded when recording the controls:

i. Preventative Control:
   Preventative Control refer to a control that is designed in such a way that it prevents the risk of non-compliance from occurring.

ii. Detective Control:
   Detective Control refer to a control that is designed in such a way that it detects the non-compliance after the event of non-compliance occurred.

iii. Corrective Control:

Corrective Control refer to a control that is designed to correct errors or irregularities that have been detected.

An ideal adequate control should be both economical and efficient. For a control to be economical, the cost of implementing the control should be equal to, but not greater than the benefit derived from the control. Many regulatory requirements however require of CoE to implement controls irrespective of the cost to the organisation. CoE must as far as is possible opt for the most economic manner in which to implement a control to provide for reasonable assurance that the compliance risk is addressed. For a control to be efficient, the control must reduce the probability of non-compliance to a level that is acceptable to the CoE.

.

2.1.3.8. Responsible Person:

The person/s responsible for the controls is recorded in the Compliance Risk Management Plan. The responsible person/s can be identified by name and/or designation.

2.1.3.9. Target Date:

The dates for implementation of the controls are recorded in the Compliance Risk Management Plan if the controls are not already implemented. If the controls are already implemented, the target date is indicated as 'In Place'.

The Compliance Risk Management Plans are distributed to the department to assist them with the active management of their compliance risks. The compilation/updating of the Compliance Risk Management Plans are an important deliverable in the implementation of an economic and efficient Compliance Risk Management Framework, serving as a management tool to the departments.

2.1.3.10. Compliance Awareness

Compliance Awareness activities are undertaken to enhance the compliance culture within CoE and can consist of one or more of the following examples of activities:

a) Involvement in the New Employee Orientation Programme.
b) Contributions to in-house publications.
c) Campaigns/newsletters.
d) Legal Updates

2.1.3.11. Compliance Checklists

Compliance checklists refer to questionnaires that are drawn up to ascertain whether or not CoE processes are compliant to a piece of Legislation or Regulation. The process followed in rolling out Compliance Checklists is:

a) Ascertain whether or not legislation is applicable to a Department.
b) Establish whether, through the Compliance Risk Profiling process, the Legislation is rated as High Risk for the Department.
c) Pull out focussed questions from the procured Checklist that apply specifically to a Department.
d) Forward Checklist to Department and agree on completion date with the GRC champion in that department.
e) Review and authenticate the responses received from the Department to ascertain current level of compliance then.
f) Workshop Departmental controls for non-compliant issues; and
g) Track and report on progress in executing the controls as agreed.

2.1.3.12. Compliance Training

Compliance Training is provided and/or facilitated in respect of:

h) The compliance methodology.
i) Regulatory requirements.
j) Significant compliance risks.

2.1.4. Phase 4 – Compliance Risk Monitoring

The Internal Audit Department together with Risk Management Department are responsible for providing the Council, Mayoral Committee, the City Manager, and management with independent assurance in respect of the adequacy and effectiveness of the regulatory control environment implemented by each department to mitigate and manage the compliance risks they are exposed to.

From a monitoring perspective it is not always practical and/or cost-effective to monitor all of the regulatory requirements applicable to a department. Priority is therefore given to the monitoring of regulatory requirements prioritised as Level 3, Level 4, Level 5 regulatory requirements. Monitoring is conducted in accordance with a three-year strategic rolling plan as compiled by the Internal Audit function and discussed and agreed with the head of each department or his/her nominee. The three-year strategic rolling plan will indicate the regulatory requirement/s that will be monitored as well as the frequency of monitoring that will be undertaken.

The Compliance function will be responsible for undertaking ad hoc monitoring exercises in respect of significant risks as identified and agreed upon with the relevant Heads of Department. The following types of monitoring are conducted:

i. Control Adequacy Reviews.
ii. Control Effectiveness Reviews.
iii. Management Control Self-Assessment Questionnaires/Sign-offs.
iv. Control Spot Check Reviews.

2.1.4.1. Control Adequacy Reviews

Control Adequacy Reviews are conducted to determine whether a control exists (test for existence involves selecting one item from a population) and whether the control is efficient (whether the control reduces the impact and probability of non-compliance to a level that is acceptable to CoE and the department management).

Control Adequacy Reviews can be conducted as part of the compilation of the Compliance Risk Management Plan (in which case a Compliance Planning Memorandum will not be issued) or it can be conducted at the same time that the Control Effectiveness Reviews are undertaken (in which case the Compliance Planning Memorandum issued for the Control Effectiveness Review must state that a Control Adequacy Review will be undertaken simultaneously).

Prior to conducting a Control Adequacy Review, an audit program must be compiled. The audit program lists the review steps (test) to be performed by the Internal Audit department. The Compliance Risk Management Plan can be utilised to document the audit program, by adding an extra column for the audit program or the Control Adequacy Review can be utilised to document the audit program.

The performed control adequacy test is documented in the Control Adequacy Review Working Paper which serves as confirmation of the work performed, the information gathered, and the conclusion reached. Evidence gathered throughout the review must be kept record of and if not able to keep record,

the evidence must be identifiable and retrievable. To the extent possible copies must be made of inaccurate and/or incomplete documents and kept record of to ensure that no disputes occur at a later stage regarding the accuracy and correctness of the finding. Methods that can be utilised to obtain evidence of adequacy include:

Method	
Interview	Consulting with an employee to understand how a control functions, e.g., asking whether gifts received are documented in a Gifts Register.
Observation	Viewing a process and procedure, e.g., sitting in on a disciplinary hearing to see whether the correct questions are asked to ensure that dismissals meet the process and procedure requirements.
Re-performance *	Re-performing a control that was executed, e.g., recalculating the solvency ratio as prescribed by legislation.
Vouching/Verification *	Compare/Confirm the information provided to a source document, e.g., obtaining the Minutes of a meeting to confirm an agreement reached or confirm that a client was correctly identified by verifying his identity against a copy of his Identity Document/Passport.
Walk-through	Following a process and procedure through from its inception to its conclusion, e.g., examining the entire process and procedure of the company's annual general meeting.

***** These methods are a more reliable form of evidence as they are supported by physical evidence.

An individual control can be found to be adequate or inadequate whilst a grouping of controls can be found to be partially adequate. If a control is found to be adequate, the control does not have to be tested on an annual basis for adequacy, unless changes are affected to the design of the control in which instance the control must be tested again for adequacy. If a control is found to be inadequate or if a grouping of controls is found to be partially adequate, the finding must be logged on the Compliance Issues Log after the final Control Adequacy Review Report (inclusive of Management Comment) was distributed to the relevant stakeholders. The relative importance of the finding is indicated by rating the finding as High, Medium, or Low:

Rating	**Description**

High	Non-adherence may threaten the continued viability of business due to a material impact on profits or market share due to severe financial loss (fines, operational losses) and/or negative publicity.
Medium	Non-adherence could have a significant impact on profits or market share due to severe financial loss (fines, operational losses) and/or negative publicity.
Low	Non-adherence could have an insignificant impact on profits or market share due to severe financial loss (fines, operational losses) and/or negative publicity.

The end-product of the Control Adequacy Review is the Control Adequacy Review Report. The report illustrates the value derived from the review and contains sufficient information to convey the required message to management but is not so detailed that the message is obscured.

2.1.4.2. Control Effectiveness Reviews

Control Effectiveness Reviews are conducted to determine whether an adequate control has been applied consistently throughout the period under review. Control Effectiveness Reviews are preferably conducted over a three-month period, as follows:

Month 1:
The first month is utilised to plan the review, to agree the scope and approach of the review with management and to compile the audit program. The scope and approach is agreed with management by compiling and distributing a Compliance Planning Memorandum. The Compliance Planning Memorandum details the purpose, objective, scope, approach, etc. Prior to conducting a Control Effectiveness Review, an audit program must be compiled. The audit program lists the review steps (test) to be performed by the Compliance Officer. The Compliance Risk Management Plan can be utilised to document the audit program, by adding an extra column for the audit program or the Control Effectiveness Review can be utilised to document the audit program. The key to a successful audit program is the use of verbs.

Month 2:
The second month is utilised to conduct the fieldwork. It is not practical or cost-effective to test whether the adequate control has been applied consistently to each and every item within the population selected; a sample that is representative of the population is therefore selected and tested, and on which basis a conclusion is reached. The norm is to test 25 items per population. If the population consists of less than 25 items, the total population must be tested. The sampling technique utilised by the Compliance Officer is dependent on the nature of the population and the objective of the test. In selecting a sample there is a statistical and a non-statistical approach of which the following sampling techniques are mostly utilised:

Statistical Sampling Approach

Interval Sampling	Selecting a sample at set intervals, for example every tenth item.
Random Sampling	Selecting a sample by means of randomised tables.

Non-statistical Sampling Approach	
Haphazard Sampling	Selecting a sample manually without any specific logic.
Judgemental Sampling	Selecting a sample based on judgement.

The performed control effectiveness test is documented in the Control Effectiveness Review Working Paper which serves as confirmation of the work performed, the information gathered, and the conclusion reached. Evidence gathered throughout the review must be kept record of and if not able to keep record, the evidence must be identifiable and retrievable. To the extent possible copies must be made of inaccurate and/or incomplete documents and kept record of to ensure that no disputes occur at a later stage regarding the accuracy and correctness of the finding. Methods that can be utilised to obtain evidence of effectiveness include:

Method	
Re-performance	Re-performing a control that was executed, e.g. reconciling the number of money-laundering reports received from the business units with the number of money-laundering reports submitted to the South African Police Service.
Vouching/Verification	Compare/Confirm the information provided to a source document, e.g. comparing the amount of penalties paid as reflected on the general ledger account with the penalty statement received from the South African Revenue Services.

A control can be found to be effective (≥ 90%), partially effective (≥70% <90%), or ineffective (<70%). If a control is found to be partially effective or ineffective, the finding must be logged on the Compliance Issues Log after the final Control Effectiveness Review Report (inclusive of Management Comment) was distributed to the relevant stakeholders. The relative importance of the finding is indicated by rating the finding as High, Medium, or Low:

Rating	**Description**
High	Non-adherence may threaten the continued viability of business due to a material impact on profits or market share due to severe financial loss (fines, operational losses) and/or negative publicity.
Medium	Non-adherence could have a significant impact on profits or market share due to severe financial loss (fines, operational losses) and/or negative publicity.
Low	Non-adherence could have an insignificant impact on profits or market share due to severe financial loss (fines, operational losses) and/or negative publicity.

Month 3:
The third month is utilised to discuss the findings with management, to agree the corrective action plan and to finalise the report. The end-product of the Control Effectiveness Review is the Control Effectiveness Review Report. The report illustrates the value derived from the review and contains sufficient information to convey the required message to management but is not so detailed that the message is obscured.

2.1.4.3. Control Spot Check Reviews

Control Spot Check Reviews are conducted to determine whether the adequate control has been applied consistently throughout the period under review. The difference to a Control Effectiveness Review is however that the scope of a Control Spot Check Review does not encompass the majority of applicable provisions of a regulatory requirement but is limited to specific selected provision/s (area of concern) of a regulatory requirement. Control Spot Check Reviews are usually undertaken as a result of information picked up from sources such as newspaper articles, internal and external audit reports, requests by management, etc.

2.1.4.4. Management Control Self-Assessment Questionnaires/Sign-offs

Management Control Self-Assessment Questionnaires/Sign-offs are conducted as a form of monitoring, utilised to assist the department in validating the existence/non-existence and effective/ineffective operation of the regulatory control environment by means of a formal declaration in order to highlight the control deficiencies that require management's attention. Management Control Self-Assessment Questionnaires/Sign-offs is obtained from employees who are accountable for the regulatory control environment and/or responsible for the control/s. The annual Compliance Certification falls within the ambit of this type of monitoring.

2.1.4.5. Compliance Issues Log

The compliance issues/findings raised are logged in the Compliance Issues Log whereof the purpose is:

i. to provide for a means by which the compliance issues/findings can be tracked to ensure that the compliance issues/findings are resolved successfully and timely.
ii. to provide for a means by which trend analysis can be conducted regarding the most common compliance issues/findings occurring group-wide; and
iii. to provide for a means to streamline the reporting of the compliance issues/findings to the relevant governance committees.

The Compliance Issues Log should contain enough information to ensure that the compliance issues/findings are not overlooked but should not be so detailed that visual scanning becomes difficult. The Compliance Issues Log is updated on a quarterly basis.

2.1.4.6. Investigations

The Internal Audit function conducts investigations in respect of calls and reports received from the Ethics Line where impacting on a compliance risk. Reported matters are dealt with accordingly:

i. The anonymity of a caller is respected and protected. If a caller makes known its identity, his/her identity is treated with the appropriate confidentiality, unless the caller agrees to make known his/her identity and is prepared to testify, if so called upon to do.
ii. Valid disclosures are investigated and acted on in a timely manner.
iii. Callers who have made a valid protected disclosure are protected against victimisation in the workplace and should be protected from occupational detriment and retaliation. If a caller is victimised or concerned about potential victimisation must the caller, the Compliance function in which instance the Compliance function will notify the Legal Advisor for assistance.

The conducting of monitoring is an important deliverable in providing assurance to the Council, Mayoral Committee, City Manager and management regarding the adequacy and effectiveness of the regulatory control environment implemented by each department to mitigate and manage the compliance risks they are exposed to.

2.1.5. Phase 5 – Compliance Risk Reporting

The Compliance Function reports on the status of the management and mitigation of the compliance risks by means of:

i. Compliance Review Reports from Risk Management Department:
Compliance Review Reports provide the SMT, Risk Management Committee, Audit Committee, City Manager, Council and Mayoral Committee, with independent assurance on the adequacy and effectiveness of the control environment designed and implemented by the Departments to comply with applicable regulatory requirements.

ii. Legal Compliance Reports from Corporate Legal:
Legal compliance reports should highlight all legislative updates on new and/or amended legislation, possible amendments to the regulatory landscape; upcoming training or workshops, legal awareness and research and advice on possible regulatory risks to CoE.

iii. Quarterly Compliance Reports from Departments:
Quarterly departmental compliance reports provide the CoE management with detailed information, highlighting matters of achievement, importance, and concern in respect of the department's management of compliance risks.
Quarterly GRC and Risk Committee Reports provide the relevant committees and the Board with summarised information in respect of CoE's management of compliance risks, highlighting matters of achievement, importance, and concern in respect of the individual departments.

2.1.5.1. Record keeping

Record keeping is an important on-going activity. Compliance related records should be stored in a manner that ensures that they are safe from destruction. Record must be up to date, legible, readily identifiable and easily retrievable. The compliance function records will be stored and retained in line with the CoE's records management policy.

The Governance, Risk and Compliance system will also be used for maintaining records of information gathered during the monitoring processes.

2.1.5.2. Conclusion

The methodology developed and implemented by CoE Compliance function is aligned with standard risk management practices, the Compliance Institute of South Africa's Generally Accepted Compliance Practice Framework, King IV (and various other regulatory requirements) and best practice.

The Compliance Framework promotes self-sustaining levels of operations that minimise and mitigates the compliance risks CoE is faced with by ensuring that the compliance risks have been identified, assessed, managed, monitored and reported on in a structured way.

3. SUPPORTING CLAUSES

Provisions of this framework are consistent with **CoE's Compliance Policy**, the scope of application, definitions and referential applicability of relevant acts, policies, regulations and guidelines are also consistent with the **CoE's Compliance Policy** that was developed in terms of this clause, except where specifically stated.

3.1. SCOPE OF APPLICATION

This framework shall apply uniformly to all employees throughout the COE. Each COE employee and stakeholder is required to know and understand this framework and its relevance for his/her function.

3.2. DEFINITIONS

Term	Description
"CoE"	*means the City of Ekurhuleni*
"Employee"	*means a person in the employ of the CoE or an Entity of the CoE*
"Councillor"	*means active Councillor of the CoE*
"Council"	*means the legally constituted Council of the CoE.*
"Structures Act"	*means the Municipal Structures* Act, Act 117 of 1998 and the regulations promulgated in terms thereof.
"Systems Act"	means the Local Government: Municipal Systems Act, Act 32 of 2000 and the regulations promulgated in terms thereof.
IDP	*Means Integrated Development Plan*
ICT	*Means the Information, Communication and Technology department*
CEO	*Means the Chief Executive Officer of an Entity; may be referred to as the Managing Director. The title refers to anyone who is the Accounting Officer*

3.3. REFERENTIAL APPLICABILITY

This Compliance Framework should be read in conjunction with the following policies, procedures and relevant statutes, including but not limited to:

Description	Context and relevance
Municipal Finance Management Act, no 56 of 2003	Details the financial arrangements prescribed for Municipalities
Municipal Systems Act	Legal authority of Municipality to regulate their operations through policies
Companies Act, 73 of 2008	To ensure that the Governance structures within the Entity are aligned with the Companies Act
KING IV Report on Corporate Governance	To align the CoE entities with industry best practice

4. ACCEPTANCE

This document has been seen and accepted by:

Name	Designation	Capacity
Risk Management Department	Governance and Compliance Management	Drafter of the policy
Governance Risk and Compliance Forum	Departmental Governance Risk and Compliance practitioners	Departmental GRC representatives
Senior Management Team (SMT)	Heads Of Departments	Policy custodians
Corporate Legal Services	DH: Corporate Legal Services	Vetting
Risk Management Committee (RMC)	Risk Management Committee	Recommend to Council for approval

5. REVISIONS

Date	Rev.	Remarks
August 2015	1st	Last approved in 2015
March 2025	2nd	In line with the CoE review guidelines: once in three years.

6. APPROVAL

This CoE's Compliance Framework is hereby approved for and on behalf of the CoE.