OVERBERG DISTRICT MUNICIPALITY

ENTERPRISE RISK MANAGEMENT POLICY

Version 9

Contents

Overberg District Municipality's Policy statement

Risk management is recognised as an integral part of responsible management and the Municipality therefore adopts a comprehensive approach to the management of risk. The Overberg District Municipality is committed to the optimal management of risk in order to achieve our vision, service delivery and strategic key objectives to ensure appropriate outcomes for the community.

All risk management efforts will be focused on supporting the Municipality's objectives. Equally, they must ensure compliance with relevant legislation and fulfil the expectations of employees, communities and other stakeholders in terms of good corporate governance.

Commitment to risk management is a sure expression of commitment to Batho Pele principles. The Overberg District Municipality is committed to a process of risk management that is aligned to the principles of leading practice and legislation, e.g. Municipal Finance Management Act (MFMA) and the King V Report on Codes of Governance. It is required that all directorates will follow a uniform risk management process and align processes to its key principles and objectives.

Risk in the Overberg District Municipality is a complex and diverse concept. It is the intention that all departments will work together in a consistent and integrated manner, with the overall objective of reducing risk and optimizing opportunities, as far as reasonably practical in the interest of the municipality.

The Council recognizes the wide range of risks to which the Overberg District Municipality is exposed. It is therefore a strategic objective to adopt a process of Enterprise risk management (ERM) that will assist the Overberg District Municipality in meeting its key goals, most specifically:

- To align the risk-taking behaviour to better achieve the goals and related objectives;
- To protect the reputation and brand name of the Overberg District Municipality;
- To promote a risk awareness ethics in all Departments/Directorates and improve risk transparency to stakeholders;
- To maximise (create, protect and enhance) stakeholder value and net worth by managing risk that may impact on the development and success indicators;
- To identify risk improvement opportunities that will maximise business opportunities and sustainable delivery of services and programs.

Effective risk management is imperative to the municipality, with its diverse key processes and an intrinsic risk profile. The realisation of the municipality's Integrated Development Plan (IDP), strategic goals and objectives depends on all role-players being able to take calculated risks in a way that does not jeopardise service delivery. Sound management of risk will enable all role-players to anticipate and respond to the changes in our environment, as well as to make informed decisions under conditions of uncertainty and inherent risk.

Management is responsible for ERM execution, in the achievement of the Overberg District Municipality's IDP strategy and every employee, partner, contractor and specialist has a part

to play in this important endeavour and we look forward to working with you in achieving these goals.

1. PURPOSE AND SCOPE

1.1 Purpose

The purpose of this policy is to formalise The Overberg District Municipality's Enterprise Risk Management (ERM) program and to articulate the roles and responsibilities of the risk implementers, oversight bodies, and risk management and assurance providers in risk management. Through this policy the Overberg District Municipality puts into practice its commitment to implement risk management and embed a culture of risk management within the municipality. This policy forms the basis for the accompanying risk management strategy which is designed to help achieve the objectives of implementing an effective ERM process.

1.2 Scope

The scope of this policy applies throughout the Overberg District Municipality in as far as risk management is concerned.

Sound risk management principles must become part of routine management activity across the municipality. The key objective of this policy is to ensure the municipality has a consistent basis for measuring, controlling, monitoring and reporting risk across the municipality at all levels.

1.3 Policy Objectives

The objectives of this policy are -

[a] to provide a framework for the effective identification, measurement, avoidance / management and reporting, of the Municipality's risks;

[b] to define and assign risk management roles and responsibilities within the Municipality; and

[c] To define a reporting framework which ensures regular communication of risk management information to the Council, portfolio committees, the Audit and Performance Audit Committee and senior management and officials engaged in risk management activities.

2. DEFINITIONS

In this policy, unless the context indicates otherwise, a word or expression, to which meaning has been assigned in the Municipal Finance Management Act (MFMA) and the Local Government Risk Management Framework, has the same meaning.

In interpreting the under-mentioned definitions, cognisance must also be taken of the definitions as encapsulated in applicable enabling legislation and framework.

Accounting Officer refers to the Municipal Manager.

Control: Control activities are the policies and procedures that help ensure that management's risk responses are carried out. Control activities occur throughout the municipality, at all levels and in all functions. They include a range of activities as diverse as approvals, authorisations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

Combined Assurance: A process that seeks to optimise the scope of assurance to the ODM by harmonising the work of various providers of assurance through eliminating fragmentation and duplication of efforts.

Council: The Municipal Council as referred to in section 18 of the Municipal Structures Act, and as defined in section 1 of the MFMA.

Corruption: The giving or offering, receiving or agreeing to receive, obtaining or attempting to obtain any benefit which is not legally due to or by a person who has been charged with a duty or power by virtue of any employment, to do any act or omit to do any act in relation to that power or duty.

Current Controls: Existing controls that are currently embedded in the department / directorate / municipality. The controls have already been designed and implemented.

Enterprise-wide Risk Management: A systematic, co-ordinated and inclusive process which uses the Institution's strategy and objectives as the focal point to manage the range of risks and optimisation of opportunities to enhance the achievement of the strategy and objectives.

Event means an incident or occurrence from internal or external sources that affects the achievement of the municipality's objectives.

Fraud: An unlawful and intentional making of a misrepresentation, which is prejudicial or potentially prejudicial to another. The term is used to describe acts such as deception, bribery, forgery, extortion, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts, collusion etc.

Impact means a result or effect of an event. The impact of an event can be positive or negative.

Incident: A risk that has actualised.

Inherent refers to the impact that the risk will have on the achievement of objectives if the current controls in place are not considered.

Key risks – Risks that are rated high on an inherent level. It is risks that pose a serious threat to the municipality.

Likelihood / Probability means the probability of the event occurring.

Management refers to all levels of management, other than the Municipal Manager and the CRO.

Mitigation / Treatment – After comparing the inherent risk score with the risk appetite and tolerance, risk with unacceptable levels of risk will require treatment plan (additional action to be taken by management). (Addressing the cause, impact and/or likelihood of the risk, to either decrease or increase the risk level to below the risk appetite of the Municipality).

Operations are a term used with "objectives", having to do with the effectiveness and efficiency of the Municipality's activities, including performance and safeguarding resources against loss.

Residual Risk means the remaining exposure after the controls/treatments has been taken into consideration. (The remaining risk after management has put in place measures to control the inherent risk).

Risk The effect of uncertainty on the achievement of the Institution's IDP and SDBIP caused by the presence of risk factors; and or the failure to optimise opportunities to enhance the achievement of the IDP and SDBIP.

Risk appetite means the amount (level) of risk that municipality is willing to accept.

Risk owner means the person responsible for managing a particular risk.

Risk Register – The risk register will outline the number of risks, type of risk and potential effects of the risk. This outline will allow the municipality to anticipate additional costs or disruptions to operations.

Risk Profile – The municipality's risk management process, systems, structures, resources, data, information, staff and related activities and initiatives. In other words, the entire risk management function of the municipality.

Risk Tolerance means the level of risk that the municipality has the ability to tolerate / bear.

Risk Universe means the Municipality's risks per risk classification capered and assessed against district, provincial, national and international related industries. Overberg District Municipality's risk register is compared with the annual IRMSA Risk Report: South Africa Risks

Strategic Risk: Risks connected with strategy selection, implementation or revision which affects the achievement of the IDP. Strategic risks occur both from poor business decisions as well as the failure to effectively implement good decisions.

3. LEGISLATIVE CONTEXT

Section 195 of the Constitution emphasises the values and principles underpinning public administration, which include the efficient, economic and effective use of resources in the public sector.

Section 83 of the Municipal System Act, No 32 of 2000 "*measures must be taken around service providers that minimise the possibility of fraud and corruption"* and

Section 104 *"loss control on municipal equipment be minimized thereby reducing the possibility of fraud and corruption and that this will be regulated by the Municipality Executive Council".*

Section 120 of the Municipal Finance Management Act, No 56 of 2003 – Public-private partnership: "*A municipality may enter into a public-partnership agreement, but only if the municipality can demonstrate that the agreement will –*

Transfer appropriate technical, operational and financial risk to the private party."

Regulation 9 of the Municipal Supply Chain Management Regulation [Notice 868 of 30 May 2005] prescribes that the Municipality's supply chain management must describe in sufficient detail effective systems for risk management. Regulation 41 provides for the for the identification, consideration and avoidance of potential risks in the supply chain management system. The risk management provisions in the supply chain management policy must include:-

- The identification of risks on a case-base basis;
- The allocation of risk to the party best suited to manage such risks;
- Acceptance of the cost of the risk where the cost of transferring the risk is greater that retaining it;
- The management of risk in a pro-active manner and the provision of adequate cover for residual risks; and
- The assignment of relative risks to the contracting parties through clear and unambiguous contract documentation.

The Municipal Finance Management Act, No 56 of 2003, sets out the roles and responsibilities of the key stakeholders within the risk management process as follows:

- Accounting Officer: Section 62(1)(c)(i) states that the Accounting Officer takes all reasonable steps to "*… ensure that the municipality has and maintains effective, efficient and transparent systems of inter alia risk management and internal control.*"

- Management, Chief Risk Officer, Risk Specialists and Other Personnel: In terms of section 78 *"…management responsibilities are extended to all senior managers and other officials of municipalities. This implies that responsibility for risk management vests at all levels of management and personnel and is not limited to only the Municipal Manager, the Risk Management Unit or Internal Audit Division".*

- Internal Audit: Section 165 of the MFMA requires that:
  "(2) The internal audit unit of a municipality or municipal entity must –
  (a) Prepare a risk based audit plan and an internal audit program for each financial year;
  (b) *Advise the accounting officer and report to the Audit and Performance Audit Committee on the implementation on the internal audit plan and matters relating to:*
  (iv) Risk and risk management."

- Audit and Performance Audit Committee: Section 166 (2) of the MFMA states:
  "(2) An Audit and Performance Audit Committee is an independent advisory body which must–
  (a) Advise the municipal council, the political office-bearers, the accounting officer and the management staff of the municipality, or the board of directors, the accounting officer and management staff of the municipal entity, on matters relating to -
  (ii) Risk management"

3.1 Applicable Frameworks

The following frameworks guides the risk management practices of Municipality:

- The Public Sector Risk Management Framework (PSRMF) by National Treasury provides a generic guide for the implementation of risk management strategies in the public service, and suggests that risk management is a formal step-by-step process that can be applied at all levels of a Department. Local Government Risk Management Framework devolves from the Public Sector Risk Management Framework.

- These principles need to be implemented within the context of each Department who should implement this framework in the development of their own risk management strategies.

- The King V Code of Governance for South Africa has thirteen principles to be applied and each are of equal importance and together forms a holistic approach to governance. The Governance of Risk (principle 8) is one of these focus areas and in turn is broken up into governance elements, and recommended practices.

- COSO Committee of Sponsoring Organizations of the Treadway Commission is focusing in Integrating the strategy and performance of the enterprise risk management.

4. PROFICIENCY AND DUE PROFESSIONAL CARE

Risk management activities must be performed with proficiency and due professional care.

The CRO and risk champions:

Should apply the care and skills expected of reasonably prudent and competent risk management officials.

- Must exercise due professional care by considering the cost of managing the risk in relation to the value of the objective, that management define and implement controls to manage risk and reducing the probability of significant errors, irregularities or non-compliance.
- Must be alert to the significant risks that might affect objectives, operations or resources, but cannot guarantee that all significant risks will be identified.
- Should enhance their knowledge, skills and other competencies through continuing professional development. This is an interactive process and it is expected to develop as risk management matures and becomes embedded within the municipality.

5. MUNICIPALITY'S RISK MANAGEMENT APPROACH

The Overberg District Municipality's risk management approach is set out as follows:

- Rigorous risk assessment process;
- Formalised risk register;
- Monthly monitoring;
- Regular reporting;
- Data analysis; and
- Informed decision making accompanied by substantiated verification.

6. ROLE-PLAYERS IN RISK MANAGEMENT PROCESS

Every employee is responsible for executing risk management processes and adhering to risk management procedures arranged by the organisation's management in their areas of responsibilities.

6.1 Risk Management Oversight

Council

The Municipal Council takes an interest in risk management to the extent necessary to obtain comfort that properly and functioning system of risk management are in place to protect the Overberg District Municipality against significant risks.

Audit and Performance Audit Committee (APAC)

The APAC is an independent committee responsible for oversight of the Municipality's control, governance and risk management. The APAC primary responsibility is providing and independent and objective view of the effectiveness of the Municipality's risk management process. (Section 166 of the MFMA)

Fraud and Risk Management Committee (FARMCO)

The members of the FARMCO are appointed by the Municipal Manager and consists of Directors (members), Manager: IDP/Communications, Manager Performance and Risk Management, - Chief Risk Officer (invitee), the Chief Audit Executive (invitee), Municipal Manager (Invitee) and the role is to review the risk management progress and maturity of the Municipality, the effectiveness of risk management activities, the key risks facing the Municipality and the responses to address these key risks.

Mayor
The role of the Mayor is to oversee the risk management process and administration of the Municipality and convey any concerns or suggestions to the Municipal Manager,

6.2 Risk Management Implementers

Municipal Manager
The Accounting Officer is ultimately responsible for risk management within the Municipality. By setting the tone at the top, the Accounting Office promotes accountability, integrity and other factors that will create a positive control environment and support ERM.

Senior Managers (Risk Owners
Senior Managers support the Municipality's risk management philosophy, integrating it into operational routines of their directorates. They are also the risk owners and ultimately accountable for the risk management of the risks in their directorates and must therefore monitor the risk management activities within their areas of responsibility and intervene where necessary.

Risk Champions (Management)
The Risk Campion's primary responsibilities are to intervene when risk management efforts are being hampered and to provide guidance and support on the management of problematic risks and risks of a transversal nature that require the involvement of multiple people to address. Risk Champions should also assist management with the identification and mitigation of risks.

Risk Action Owners

Heads of Departments
Heads of Departments have the responsibility to integrate the risk management strategy and policy into their department's operational routines. They also implement risk actions to address operational and certain strategic risks.

Senior Staff
Senior Staff must assist their Head of Department with the implementation of risk actions. Depending on the seniority and responsibility of the staff member, some senior staff may be the actual implementers of the operational risk actions.

Employees
All employees within the Municipality have a role to play.

6.3 Risk Management Unit

The Department, Performance and Risk Management functions as the risk management unit. The risk management unit is also responsible to drive Business Continuity Framework.

Chief Risk Officer (CRO)

The Chief Risk Officer as appointed by the Accounting Officer. The CRO is the custodian of the risk management strategy and coordinator of risk management activities throughout the Municipality.

The primary responsibilities of the CRO are to bring to bear his/her specialist expertise to assist the Municipality to embed risk management and leverage its benefits to enhance performance.

Administrative Support
Administrative support with regards to risk management will be provided by the Risk Management department.

6.4 Risk Management Assurance Providers

Internal Audit
The core role of Internal Audit in risk management is to provide an independent, objective assurance to the Municipal Manager, Municipal Council, Fraud and Risk Management Committee and the Audit & Performance Audit Committee on the effectiveness of risk management.

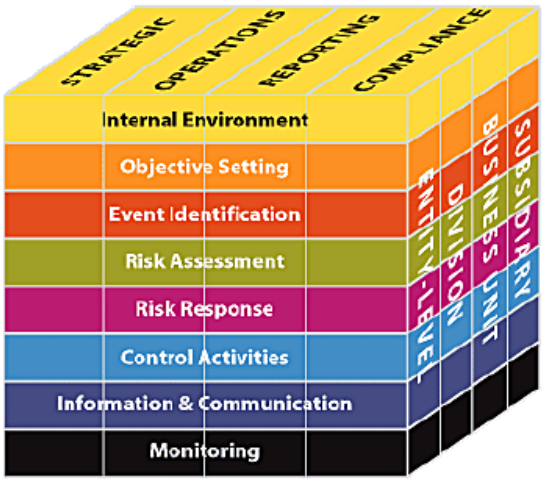
Internal Audit also assists in bringing about a systematic disciplined approach to evaluate and improve the effectiveness of the entire system of risk management and provide recommendations for improvement where necessary. Internal Audit must determine whether the risk management process is efficient and effective.

Auditor-General
The Auditor-General provides an independent opinion on the effectiveness of risk management. In providing an opinion the Auditor-General focuses on:

- Determining whether the risk management strategy, policy and implementation plan are in place and appropriate;
- Assessing the implementation of the risk management strategy, policy and implementation plan;
- Reviewing the risk assessment process to determine if it is sufficiently robust to facilitate timely and accurate risk rating and prioritisation;
- Determining whether management action plans to mitigate the key risks are appropriate and being implemented effectively.

7. ENTERPRISE RISK MANAGEMENT PROCESS

The enterprise risk management process comprises eight (8) components:



Enterprise Risk Management Process (COSO ERM Framework)

Internal Environment

The Internal environment encompasses the tone Overberg District Municipality, influencing the risk consciousness of its people. It is the foundation for all other components of risk management, providing discipline and structure.

Ethics

The effectiveness of risk management activities is directly influenced by the ethical behaviour of the people responsible for risk management, which included their professionalism and commitment in executing their risk management responsibilities.

A lack of ethic is a contributing factor to a variety or risks, either being the cause of the risk itself or the cause of ineffective control measures. Therefore, risk management initiatives can only be successful in an environment of ethical behaviour with adequate ethics risk management process.

Overberg District Municipality has a Code of Ethics for Municipal Staff and Councillors in place to regulate the conduct and ethical behaviour expected in the workplace.

7.1 Authority

Risk Management Unit

The Risk Management Unit has the authority to conduct all activities listed in the approved risk management implementation plan and executions from the FARMCO and Municipal Manager.

The Risk Management Unit may respond to requests for assistance received from the Municipal Manager, Senior Managers and Managers. Requests for assistance from other staff must first be approved by their manager.

Internal Audit

Internal Audit has the authority to investigate/audit any matter that is included in the approved risk-based audit plan or requested by the Municipal Manager or APAC.

Fraud and Risk Management Committee (FARMCO)
The FARMCO terms of reference is approved by the Municipal Council. The FARMCO is thus authorised to conduct all activities listed in the FARMCO Terms of Reference.

Audit and Performance Audit Committee (APAC)
The APAC has by law the authority to conduct all activities listed in Section 166(2) and (3) of the MFMA. Additionally, the APAC has the authority to conduct all activities contained in the APAC Charter approved by the Municipal Council.

7.2 Risk Identification

All activities undertaken by the Municipality, both existing and emerging, must be assessed in order to identify any material current or emerging risks which: -

- threaten the achievement of the Municipality's objectives; or
- may cause material loss or damage to the Municipality's resources; or
- may have potentially disruptive influence on the Municipality's business continuity; or
- May impair the Municipality's reputation among its stakeholders.
- Identifying possible "Black Swan" Events – Very Rare and unpredictable events that may have catastrophic consequences or a devastating impact on the operations or sustainability of the Municipality (This assessment may also include "*Incident*" and Emerging risks).

For this purpose, the Municipal Manager and departmental heads must utilise the risk identification and assessment matrix included in this policy.

Risk Description
There are numerous definitions of risk, which are informed principally by the context in which they are applied.

The following is a commonly used definition: "*A risk is any threat or event that is currently occurring, or that has a reasonable chance of occurring in the future, which could undermine the institution's pursuit of its goals and objectives.*"

Risks manifest as negative impacts on goals and objectives or as missed opportunities to enhance institutional performance. Stakeholders expect the Municipality to anticipate and manage risks in order to eliminate waste and inefficiency, reduce potential shocks and crises and to continuously improve capacity for delivering on their institutionalised mandates.

A short, short to the point description of the risk must be articulated. For ease, the cause of risk should be established first and secondly the background information related to the risk. The risk description can then be articulated using the cause and background information.

Cause of Risk
Current and/or potential causes of the risk must be established and included in the risk register.

Risk Background
Supplementary and/or explanatory information is required to enable users of the risk reports some of whom has no knowledge about the risk, to understand the risk.

Consequences
The potential consequences should the risk materialise must be identified and included in the risk register.

Risk Classification.
After the risk has been identified, it can be classified according to its nature.

Overberg District Municipality classifies risks in accordance with the regulations and frameworks applicable to government institutions.

- Risk Types

The Municipality can be exposed to different types of risks which may be internal or external to the Municipality.

Internal risk are risks emanating from within the Municipality and over which the Municipality to a large extent has control over its occurrence.

External risks are risks emanating from outside the Municipality and the Municipality has little or no control over its occurrence.

- Risk levels

Risks have been arranged into five main levels:

Municipal Risk Levels	
Strategic risks	Strategic objectives are high-level goals aligned with and supporting the municipality's mission and vision. Strategic objectives reflect management's efforts as to how the municipality will look to create value for its stakeholders. Strategic risks are those events, which could have a negative effect on the achievement of this municipality's strategic objectives as noted in the IDP.
Operational risks	Risks that affect the achievement of the SDBIP, mainly resulting from inadequate or failed internal processes, actions of staff, loss of key personnel, failure of IT systems, failure of equipment, the actions of regulatory authorities, customers, suppliers and the public, as well as other external events that impact on the objectives. Operational risks are those events that may affect the achievement of the directorate's operational objectives.
Emerging	Newly developing or changing risks which are difficult to quantify and which may have a major impact on the municipality.

risk	
Project risk	Risks identified during the setup of the business implementation plan of a capital project or any other projects / plans, including those that has a substantial financial impact on the municipality
Incident risk	Is a risk that may come to light/ incidentally occur during the financial year but was not captured in the initial risk register for that particular financial year.
Fraud Incident risk	It is expected for any instances of fraud and corruption to be reported to FARMCO and to be followed up by the Internal Audit to identify control weaknesses or any type of process deficiencies. The identified unforeseen risks will be captured in the Risk Register. The nature and impact of the risks will indicate how the risks will be classified (Strategic or Operational). These risks relate to illegal or improper acts by employees resulting in a loss of the Municipality's assets or resources.

-Risk Category

Risks are categorised based on their origin and the area they affect:

As the risk environment is varied and complex it is useful to group potential events into risk categories. By aggregating events horizontally across an institution and vertically within operational units, management develops an understanding of the interrelationship between events, gaining enhanced information as a basis for risk assessment.

The main categories to group individual risk exposures are as follows:

Risk type	Risk Category	Description
Internal	Human resources	Risks that relate to human resources of an institution. These risks can have an effect on an institution's human capital with regard to: • Integrity & Honesty; (Ethics) • Recruitment; • Skills & competence; • Employee wellness; • Employee relations; (Labour Relations) • Retention; and • Occupational health & safety
	Knowledge and information management	Risks relating to an institution's management of knowledge and information. In identifying the risks consider the following aspects related to knowledge management: • Availability of information; • Stability of the information; • Integrity of information data; • Relevance of the information; • Retention; and Safeguarding

Internal	Litigation	Risks that the institution might suffer losses due to litigation and lawsuits against it. Losses from litigation can possibly emanate from: • Claims by employees, the public, service providers and other third parties; • Failure by an institution to exercise certain right that are to its advantage • Costs of litigation (Legal fees and productivity)
	Loss \ theft of assets	Risks that an institution might suffer losses due to either theft or loss of an asset of the institution.
	Material resources (procurement risk)	Risks relating to an institution's material resources. Possible aspects to consider include: • Availability of material; • Costs and means of acquiring \ procuring resources; • The wastage of material resources
	Information Technology	The risks relating specifically to the institution's IT objectives, infrastructure requirement, etc. Possible considerations could include the following when identifying applicable risks: • Security concerns; • Technology availability (uptime) • Applicability of IT infrastructure; • Integration / interface of the systems; • Effectiveness of technology; and • Obsolescence of technology
	Third party performance	Risks related to an institution's dependence on the performance of a third party. Risk in this regard could be that there is the likelihood that a service provider might not perform according to the service level agreement entered into with an institution. Non-performance could include: • Outright failure to perform • Not rendering the required service in time; • Not rendering the correct service; and • Inadequate / poor quality of performance.
	Occupational Health & Safety	Risks from occupational health and safety* issues e.g. injury on duty; outbreak of disease within the institution, mental trauma, adequacy and availability of protective clothing and equipment. • Risks related to compliance with provisions of the Occupational Health Act will be categorised as a compliance risk.
	Disaster recovery Business continuity	Risks related to an institution's preparedness or absence thereto to disasters that could impact the normal functioning of the institution e.g. natural disasters, act of terrorism etc. This would lead to the disruption of processes and service delivery and could include the possible disruption of operations at the onset of a crisis to the resumption of critical activities. Factors to consider include:

		• Disaster management procedures; and • Contingency planning
	Compliance \ Regulatory	Risks related to the compliance requirements that an institution has to meet. Aspects to consider in this regard are: • Failure to monitor or enforce compliance; • Monitoring and enforcement mechanisms; • Consequences of non-compliance; and • Fines and penalties paid
	Fraud and corruption	These risks relate to illegal or improper acts by employees resulting in a loss of the institution's assets or resources.
	Financial	Risks encompassing the entire scope of general financial management. Potential factors to consider include: • Cash flow adequacy and management thereof; • Financial losses; • Wasteful expenditure; • Budget allocations; • Financial statement integrity; • Revenue collection; and • Increasing operational expenditure.
	Cultural	Risks relating to an institution's overall culture and control environment. The various factors related to organisational culture include: • Communication channels and the effectiveness; • Cultural integration; • Entrenchment of ethics and values; • Goal alignment; and • Management style.
Internal	Reputation	Factors that could result in the tarnishing of an institution's reputation, public perception and image.
	Service delivery	Every institution exists to provide value for its stakeholders. The risk will arise if the appropriate quality of services is not delivered to the citizens.
	Pandemic	Risks related to the outbreak of pandemic (e.g. Covid-19) which have an effect on the Business Continuity of the municipality.

Risk Type	Risk category	Description
	Economic environment	Risks related to the institution's economic environment. Factors to consider include: • Inflation; • Foreign exchange fluctuations; and • Interest rates
	Political environment	Risks emanating from political factors and decisions that have an impact on the institution's mandate and operations. Possible

External		factors to consider include: • Political unrest; • Local, Provincial and National elections; and • Changes in office bearers.
	Social environment	Risks related to the institution's social environment. Possible factors to consider include: • Unemployment; and • Migration of workers
	Natural environment	Risks relating to the institution's natural environment and its impact on normal operations. Consider factors such as: • Depletion of natural resources; • Environmental degradation; • Spillage; • Pollution; and • Disease.
	Technological environment	Risks emanating from the effects of advancements and changes in technology
	Legislative environment	Risks related to the institution's legislative environment e.g. changes in legislation, conflicting legislation.
	Service delivery	Every institution exists to provide value for its stakeholders. The risk will arise if the appropriate quality of services is not delivered to the citizens.
	Xenophobia	Risks arising from and associated with xenophobia within Overberg district

- Risk Estimation *(Risk Rating Scales)*

In this policy, risk assessment refers to the estimation: -

- of the probability of a risk event happening, which will indicate each event's estimated frequency; and
- Of the likely impact the occurrence of a specific risk event may have on the Municipality's operations and / or reputation.

A risk's impact and likelihood are separately assessed on a 5X5 scale. The inherent risk rating is calculated by multiplying the impact rating and likelihood rating of the risk. The inherent risk exposure is determined by the inherent risk rating.

- Impact

When determining the impact rating, the worst-case scenario that could materialise when there is no control intervention from the Municipality is considered. See Impact Ratings below:

Assessment	Rating	Description
Critical	5	Major financial, operational and/or reputational loss for the municipality – issues that should be addressed on Council level.
Major	4	Critical events resulting in intervention of

		executive management. Probable long-term cessation of core business activities – material at organizational level. Required Audit Committee involvement.
Moderate	3	Reduced ability to achieve business objectives – requires top management involvement.
Marginal	2	Disruption of normal operations with a limited effect on achievement of the municipalities' strategy and objectives.
Immaterial	1	No material impact on achievement of the municipalities' strategy and objectives.

- Likelihood

The Municipality utilises a 5-point scale to estimate the likelihood of a risk event happening, as follows:

Assessment	Rating	Description
Almost certain	5	The risk is already occurring, or is likely to occur more than once within the next 12 months.
Probable	4	More likely that adverse event/opportunity will occur at least once within the next 12 months.
Possible	3	Likely that adverse event/opportunity will occur at least once in the next 3 years.
Unlikely	2	Unlikely that adverse event/opportunity will occur within the next 3 years.
Rare	1	Highly unlikely that adverse event/opportunity will occur.

- Risk Profile

The completed risk identification and assessment matrix will contain the Municipality's risk profile, which will be used to -

[a] determine the Municipality's priorities for risk treatment; and
[b] determine appropriate risk treatment actions to be taken.

7.3 Risk Evaluation

When the risk analysis process has been completed, it is necessary to evaluate the risks on the following scale:

Inherent risk exposure will be evaluated as follows:

Inherent Risk Exposure	Assessment	Definition
1 to7	Low	Mostly **acceptable** - Low level of control intervention required, if any.

8 to 14	Medium	Unacceptable level of risk, except under unique circumstances or conditions - Moderate level of control intervention required to achieve an acceptable level of residual risk. (Supplementary issue)
15 to 25	High	**Unacceptable** level of risk - High level of control intervention required to achieve an acceptable level of residual risk.

Residual risks will be evaluated as follows:

	Residual Risk Exposure	Assessment	Definition
1	0-7	Low	Mostly acceptable level of residual risk - Requires minimal control improvements.
2	8 -14	Medium	Unacceptable level of residual risk - Implies that the controls are either inadequate (poor design) or ineffective (poor implementation). Controls require some redesign, or a more emphasis on proper implementation. (Supplementary issue.)
3	15 - 25	High	Unacceptable level of residual risk - Implies that the controls are either fundamentally inadequate (poor design) or ineffective (poor implementation). Controls require substantial redesign, or a greater emphasis on proper implementation.

Residual risk Heat Map matrix

Likelihood

Almost Certain (5)	**5 Supplementary issue**	**10 Issue**	**15 Unacceptable**	**20 Unacceptable**	**25 Unacceptable**
Probable (4)	**4 Acceptable**	**8 Supplementary issue**	**12 Issue**	**16 Unacceptable**	**20 Unacceptable**
Possible (3)	**3 Acceptable**	**6 Supplementary issue**	**9 Issue**	**12 Issue**	**15 Unacceptable**
Unlikely (2)	**2 Acceptable**	**4 Acceptable**	**6 Supplementary issue**	**8 Supplementary issue**	**10 Issue**
Rare (1)	**1 Acceptable**	**2 Acceptable**	**3 Acceptable**	**4 Acceptable**	**5 Supplementary issue**
	Immaterial (1)	*Marginal (2)*	*Moderate (3)*	*Mayor (4)*	*Catastrophic (5)*

Impact

Current Control effectiveness / Residual Risks

Current controls' effectiveness in mitigating risks is assessed on a 0 -1 reduction scale.
The more effective the control, the more it mitigates the inherent risk and the less is the residual risk.

The residual risk rating is calculated by multiplying the inherent risk rating with the control effectiveness rating.

The residual risk exposure is determined by comparing the residual risk rating to the risk appetite of the Municipality.

Current Control Effectiveness

The Municipality uses an effectiveness scale to estimate the effectiveness of the internal controls, as follows:

Effectiveness category	Qualitative criteria
Very effective 0.2	Controls are pro-actively managing the risk causes and impacts, mitigating the risk as much as economically possible.
effective 0.4	Controls are managing the risk causes and impacts as planned and results in effective risk mitigation.
Moderately effective 0.75	Controls are managing the risk causes and impacts to some extent but its risk mitigation is inadequate.
Ineffective 0.9	Controls do not manage the risk causes or impacts adequately, resulting in ineffective risk mitigation.
Inherent/moderate controls in place 1	Common, non-designed controls that exist in the normal course of operations (e.g. lock outside door at end of workday)

7.4 Cost of Controls

The cost of controls includes all costs associated with maintaining the current controls for the financial year. Costs associated with replacing the controls when it reaches the end of its useful life are apportioned across financial years according to the expected useful life of the control components. Implementation costs are not included in the cost of controls. The current controls are already in place and the implementation costs have been incurred in the past.

7.5 Cost of Control vs Cost of Risk

The cost of controls is adjusted for its effectiveness and compared to the financial exposure of the risk as indicated by the following formula:

Financial exposure - [cost of controls x (1 + current controls effectiveness rating)]

A positive value indicates that the cost of controls is less than the financial consequences of the risk (value creation). A negative value indicates the cost of controls is more than the financial consequences of the risk (value destruction) and a review of controls is required to align the cost of controls with the cost of risk.

7.6 Controls Cost Effectiveness

The controls cost effectiveness is calculated by comparing the value of the cost of controls vs cost of risk against the financial exposure and expressing it as a percentage.

This figure can be seen as the Municipality's return on investment in the control environment, since the Municipality is investing money to maintain the control environment and expecting a return in the form of prevented financial losses.

The controls cost effectiveness figure allows the Municipality to compare the costs of controls of risks of different magnitude to determine whether the controls are cost effective in relation to the cost of the risk. This can be used to allocate funds to improve the control environment where it will reap the most financial benefits.

In practice, where it may be impractical to perform complex calculations, risk owners should consider the implications of decisions in managing risk, that adheres to the principles of cost/benefit analysis.

Residual risk exposure

Residual Risk Rating	Magnitude	Definition
0-7	Low	Acceptable level of residual risk – Requires no or minimal control improvements. Residual risk is below or within the risk appetite level.
8-14	Medium	Unacceptable level of residual risk – Implies that the controls are either inadequate (poor design) or ineffective (poor implementation). Controls require some redesign, or more emphasis on proper implementation.
15-25	High	Unacceptable level of residual risk – Implies that the controls are either fundamentally inadequate (poor design) or ineffective (poor implementation). Controls require substantial redesign, or a greater emphasis on proper implementation. Residual risk is above the risk appetite level.

7.7 Risk Appetite and Tolerance Levels

Risk appetite:

- Enables an improved consistency of decision making at all levels through improving risk understanding;
- Provides a framework for knowingly taking risk within defined boundaries;
- Improves the ability of the Fraud and Risk Management Committee as well as the Audit and Performance Audit Committee to challenge recommendations of management by providing a benchmark of what level of risk is defined as acceptable; and
- Derives real value from the assessment of risk over and above compliance purposes.

The risk appetite decided upon should be formally considered as part of the setting of business strategy, with capital expenditure and other strategic decisions reviewed against it as they arise. The Fraud and Risk Management Committee will review the risk appetite and recommend it to Council for approval.

Risk appetite is the amount of residual risk that the Institution is willing to accept, before action is needed to reduce it. The formulation of the risk appetite is typically closely aligned to the strategic planning process and is also inclusive of budgeting, and should be reviewed by management annually, with the annual risk review.

Management shall determine the risk appetite per identified risk and submit it to the Fraud and Risk Management Committee to advice and approve the level of risk appetite.

The risk appetite should be clearly stated and articulated so that it informs management decisions.

The risk appetite is currently set as follows:32% Risk rating: 8 [Impact (5) x Likelihood (5) = 25 x 32% = 8.

The municipality should address all risks greater than or equal to a residual risk exposure rating of 8. Addressing these risks will assist the municipality to avoid exposure to losses and to manage actions that can pose a reputational risk to the municipality.

Risk Tolerance:

Risk Tolerance refers to the maximum level of amount of risk that the Municipality can bear, before actions is needed to reduce it. All risks above the municipality's risk tolerance will receive attention form the top management team until it is mitigated to below the risk tolerance level.

Risk Tolerance will be expressed in absolutes. The municipality will be making use of risk tolerance statements and quantitative risk tolerance elements. The municipality will not be crossing risk tolerance levels unless approved by the Municipal Manager and Council. The tolerance levels in terms of Fraud & Corruption related risks will however remain at zero.

7.8 Risk Treatment (Response)

It is management's decision how they will respond to risks once all the relevant risks have been assessed. The following risk responses are available:

Risk avoidance

Avoiding the risk, e.g. by choosing a different strategy or terminating the activity that produces the risk.

Preventative maintenance and timely repair of assets, a high qualitative standard of workmanship and diligent compliance with the law are some of the strategies that could be implemented to avoid risk. However, the Municipality acknowledges that in some cases the risk event must first occur before any practicable steps can be taken to avoid the risk.

Risk acceptance/retention

Accepting the risk where cost and strategy considerations rule out alternative strategies.

It may be determined that it is more practical to retain a risk even though other methods of handling the risk are available. For example, the Municipality accepts/retains the risk of loss to stationary, petrol and diesel because of the difficulty of enumerating and evaluating all of these types of assets.

The municipality is willing to accept risk which will not be actively managed. This may be because:

- The risk is beyond the municipality's control.
- All possible and rational risk control measures have been exhausted (additional risk mitigation measures are no longer available).
- Further investment of resources to mitigate risk are not justified on cost/benefit grounds.

Risk treatment

Treating the risk, e.g. by implementing or improving the internal control system

When risk cannot be avoided, the effect of loss can often be minimised in terms of frequency and severity. Thus, the municipality mitigates its losses.

Risk transfer

Transferring the risk to another party more competent to manage it, e.g. contracting out services, establishing strategic partnerships and buying insurance.

(In some cases, risk can be transferred to others, usually by contract. The most common method of risk transfer is to purchase of insurance since the policy actually shifts the financial risk of loss, contractually, from the Municipality to the insurance company)

Exploit

Exploiting the risk factors by implementing strategies to take advantage of the opportunities presented by such risk factors.

8. RISK ACTION PLAN

The action plans to reduce the risk (referred to as risk actions) are developed according to the following criteria:

Residual Risk Level	Risk Actions
High (above risk appetite	The current controls are not effective at mitigating the risk. Comprehensive action is required, which can include new controls, enforcing current controls more strictly and redesigning the systems and processes to eliminate the cause(s) of the risk.
Medium	The current mitigation of the risk is adequate, but the control environment should be improved. The current controls should be enforced more strictly and/or new controls should be implemented.
Low	Current controls should be continuously monitored and evaluated for effectiveness. Any deficiencies identified should be addressed immediately or result in the creation of an additional risk action.

The proposed risk actions must be practical. The person responsible for the implementation of the risk action, referred to as the risk action owner, must have or be able to obtain the funds, personnel, assets, skills and time required to implement the risk action.

8.1 Implementation of Risk Actions

Along with the development of the risk action, the estimated timeframe to implement the risk action must be determined. The implementation of risk actions for risks with high likelihoods or high impacts should be fast-tracked.

The risk action owner is responsible for the implementation of the risk action and can delegate responsibilities to other staff and engage with internal and external role players to successfully complete the risk action on time.

9. MONITORING

The system of enterprise risk management is monitored, and modifications made if necessary. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two.

Monthly monitoring occurs in the normal course of management activities. The Risk Management Unit monitors the enterprise risk management of the Municipality on an ongoing basis.

The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. The Risk Management Unit and Internal Audit can perform separate evaluations.

10. RISK REPORTING

Different levels within Municipality need different information from the risk management process.

The Council, other political structures and the Municipality's political office-bearers should -

- know about the most significant risk facing the Municipality;
- ensure appropriate levels of awareness throughout the Municipality;
- be informed on the process of managing risks;
- know the importance of stakeholder confidence in the Municipality; and
- be assured that the risk management process is working effectively.

Senior and Middle Management should -

- be aware of risks which fall into their area of responsibility, the possible impacts these may have on other areas and the consequences other areas may have on them;
- have performance indicators which allow them to monitor the key business and financial activities, progress towards objectives and identify developments which require intervention [e.g. forecasts and budgets];
- have systems which communicate variances in budgets and forecasts at appropriate frequency to allow action to be taken; and
- Report systematically and promptly to Fraud and Risk Management Committee any perceived new risks or failures of existing control measures.

Officials of the Municipality should -

- understand their accountability for individual risks;
- understand how they can enable continuous improvement of risk management response;
- understand that risk management and risk awareness are a key part of the Municipality's culture; and
- Report systematically and promptly to senior management any perceived new risks or failures of existing control measures.

11. RISK UNIVERSE

Every municipality must define its own risk universe. The risk universe is a collection of risks built on environmental analysis and external benchmarking; therefore, it is recommended that the Municipality must define its own risk universe.

The Overberg District Municipality uses the risk universe in the annual revision of its strategic risks against the top risks in South Africa in terms of the Institute of Risk Management South Africa's (IRMSA) annual report.

12. COMBINED ASSURANCE

Combined assurance will optimise and maximise the level of risk, governance and control oversight over the Municipality's risk landscape, by integrating, coordinating and aligning the risk management and assurance processes within the Municipality.

A Combined Assurance Model for the risks above the risk appetite will be created and updated quarterly to ensure the Municipality's most significant risks receive adequate assurance.

The combined assurance activities of the Municipality will be conducted in accordance with the Combined Assurance Policy Framework.

13. BUSINESS CONTINUITY

Business continuity is an integral part of risk management.

In the event of extended service outages caused by factors beyond the Municipality's control, the Municipality must be able to restore services to the widest extent possible in a minimum time frame.

A Business Continuity Framework is in place to direct business continuity activities and a Business Continuity Committee has been established to oversee the execution of those activities.

14. POLICY REVIEW

This policy shall be reviewed annually to reflect the current stance on risk management within the Overberg District Municipality.

15. DATE OF LAST APPROVAL

APPROVED: COUNCIL MEETING HELD 18/06/2018, ITEM A262 (Version 4)
APPROVED: COUNCIL MEETING HELD 30/06/2017, ITEM A112 (Version 3)
APPROVED: COUNCIL MEETING HELD 5/12/2016, ITEM A25 (Version 2)
APPROVED: COUNCIL MEETING HELD 25/01/2016, ITEM A332 (Version 1)
APPROVED: COUNCIL MEETING HELD 29/06//2020, ITEM A63 (Version 5)
APPROVED: COUNCIL MEETING HELD 27/03/2023, ITEM A67 (Version 6)
APPROVED: COUNCIL MEETING HELD 23/6/2023, ITEM A91 (Version 7)
APPROVED: COUNCIL MEETING HELD 30/06/2025, ITEM A74 (Version 8)
APPROVED: COUNCIL MEETING HELD 27/07/2026, ITEM A84 (Version 9)