BEAUFORT WEST MUNICIPALITY

FRAUD AND RISK MANAGEMENT POLICY 2023

Approved by council: 23 January 2017

Resolution: 8.15 5/12/2/1

Approved by Council: 31 August 2021

Resolution: 8:1 2/12/2/1

CONTENTS **Page**

1. BACKGROUND

1.1 Purpose

The policy aims to support the objectives of the Municipality to enable the implementation and maintenance of effective systems to identify and mitigate the risks that threaten the attainment of service delivery and other objectives, and optimise opportunities that enhance institutional performance.

1.2 Background or risk management

1.2.1 Government objectives and Risk Management

The concept of risk management is not new as the basic principles of service delivery (Batho Pele, 1997) clearly articulate the need for prudent risk management to underpin the achievement of municipal objectives.

Municipalities are bound by constitutional mandates to provide products or services in the interest of the public good. As no institution has the luxury of functioning in a risk-free environment, the municipality also encounter risks inherent in producing and delivering such goods and services.

Stakeholders understand this but expect Municipalities to perform without any unnecessary exposure to risk. In other words, stakeholders are averse to value erosion caused by risks that ought to be detected and avoided through prudent management actions.

The Municipal Environment is fraught with unique challenges, such as lack of capacity, lengthy decision lead times, limited resources, competing objectives and infrastructure backlogs to mention a few. Such dynamics place an extra risk management burden on the management of municipalities.

Risk management is a management tool that increases an institutions prospect of success through getting it right the first time and minimising negative outcomes. Value is maximised when institutions set clear and realistic objectives, develop appropriate strategies, understand the intrinsic risks associated therewith and direct resources towards managing such risks on the basis of cost-benefit principles. Within high performing institutions, risk management is a strategic imperative rather than an option.

1.2.2 What is risk?

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

A generic definition of risk is as follows: ***"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 shocks and crises and to continuously improve capacity for delivering on their institutionalised mandates.

1.2.3 Risk Management

Risk management forms part of management's core responsibilities and is an integral part of the internal processes of an institution. It is a systematic process to identify, evaluate and address risks on a continuous basis before such risks can impact negatively on the institutions service delivery capacity.

When properly executed risk management provides reasonable, but not absolute assurance, that the institution will be successful in achieving its goals and objectives.

1.2.4 Enterprise Risk Management

Enterprise risk management (ERM) is the application of risk management throughout the institution rather than only in selected business areas or disciplines. ERM recognises that risks (including opportunities) are dynamic, often highly interdependent and ought not to be considered and managed in isolation. ERM responds to this challenge by providing a methodology for managing institution-wide risks in a comprehensive and integrated way.

1.2.5 Risk Categories

As the risk environment is so 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:

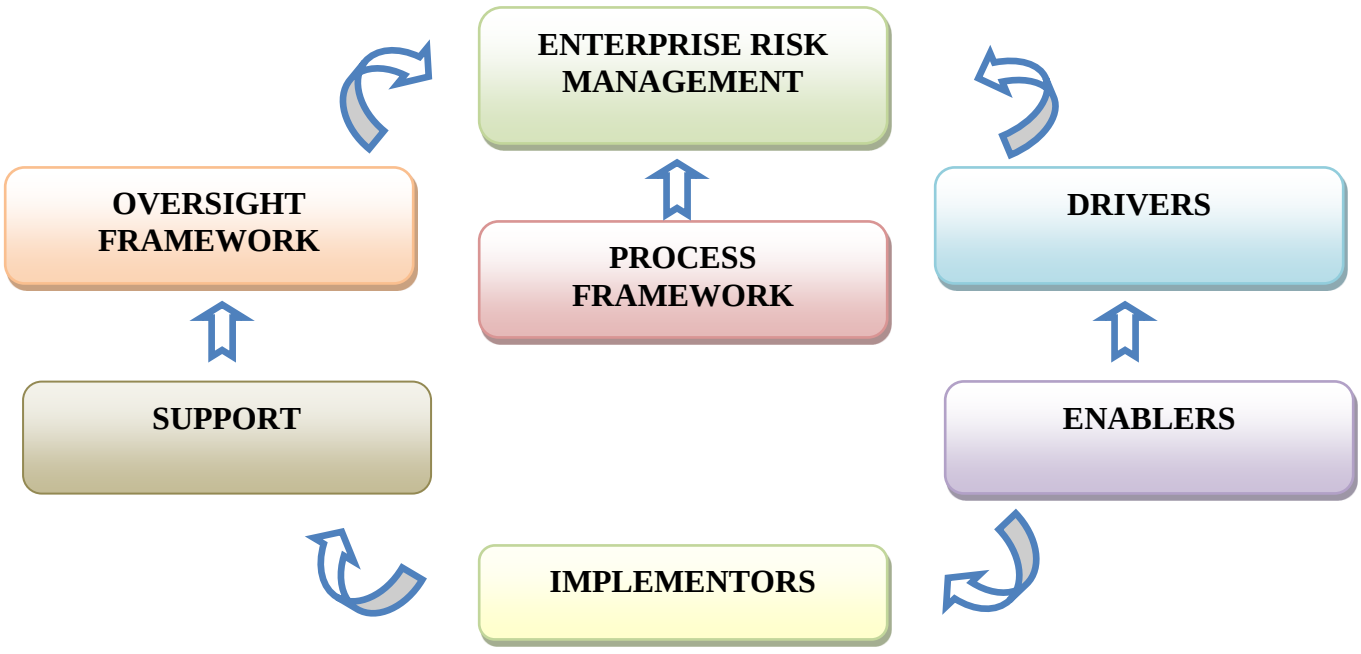
	Risk Category	**Description**
Risk type Internal	Human resources	Risks that relate to human resources of an institution. These risks can have an effect on an institution's human capital with regard to: • Integrity & Honesty; • Recruitment;

		• Skills & competence; • Employee wellness; • Employee 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
	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
	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; and • 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.
	Health & Safety	Risks from occupational health and safety issues e.g. injury on duty; outbreak of disease within the institution
	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.
	Reputation	Factors that could result in the tarnishing of an institution's reputation, public perception and image.
External	**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 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; and • Pollution
	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.



2. PROCESS FRAMEWORK

2.1 Internal Environment

The Municipality's internal environment is the foundation of risk management providing discipline and structure. The internal environment influences how strategy and objectives are established, institutional activities are structured, and risks are identified, assessed and acted upon. It influences the design and functioning of control activities, information and communication systems and monitoring activities.

The internal environment comprises many elements including an institution's ethical values, competence and development of personnel, management's operating style and how it assigns authority and responsibility.

The internal environment

- Establishes a philosophy regarding risk management. It recognizes that unexpected as well as expected events may occur. This includes activities like a risk management policy, setting of risk appetite and risk tolerance levels;
- Establishes the institution's risk culture;
- Considers all other aspects of how the institution's actions may affect its risk culture. This typically includes activities such as risk management reporting lines.

2.2 Objective Setting

Objectives must exist before management can identify events potentially, affecting their achievement. Risk management ensures that management has a process in place to both set objectives and align the objectives with the municipality's mission / vision / organisational values and is consistent with the municipality's risk appetite and tolerance levels. The setting of these objectives is usually completed during the "Strategic planning and budgetary process".

2.3 Risk Identification

The purpose of completing a risk identification exercise is to identify, discuss and document the risks facing the institution. Management almost always know what risks the institution is exposed to but they do not always formally record such risks. This necessitated the development of risk identification guidelines to ensure that institutions manage risk effectively and efficiently.

The risk identification is defined as "the process of determining what, where, when, why and how something could happen". Risk identification is a deliberate and systematic effort to understand and document all of the key risks facing the institution.

The objective of risk identification is to generate a comprehensive list of risks based on those events and circumstances that might enhance, prevent, degrade or delay the achievement of the objectives. This list of risks is then used to guide the analysis, evaluation, treatment and monitoring of key risks.

2.4 Risk Assessment

The risk assessment is a systematic process to understand the nature of risk and determine the level of risk. The risk assessment step aims to develop an understanding of the risk. It provides an input to decisions on whether risk response is necessary and the most appropriate and cost-effective risk response strategies.

The main purpose of risk assessment is to help management to prioritise the identified risks. This enables management to spend more time, effort and resources to manage risks of higher priority than risks with a lower priority.

2.5 Risk response strategy

A key outcome of the risk identification and evaluation process is a detailed list of all key risks including those that require treatment as determined by the overall level of the risk against the institution's risk tolerance levels. However, not all risks will require treatment as some may be accepted by the institution and only require occasional monitoring throughout the period.

All key risk identified should be responded to however not all these risk will require treatment. The risks that fall outside of the institution's risk tolerance levels are those which pose a significant potential impact on the ability of the institution to achieve set objectives and therefore require treatment.

The purpose of responding and treating risks is to minimize or eliminate the potential impact the risk may pose to the achievement of set objectives.

Risk response involves identifying the range of options for responding to risks, assessing these options and the preparation and implementation of response plans.

Risk response may involve a cyclical process of assessing a risk response, deciding that current risk levels are not tolerable, generating new risk response/s, and assessing the effect of that response until a level of risk based on the agreed risk criteria is reached.

2.6 Control activities

The institution can respond to risk through various mechanisms such as avoidance, transfer, accepting and managing of the risk. When the institution elects to manage the risk, it will require control activities to support the management of the risk to within tolerable levels.

The risk assessment will have produced a management's perspective of the effectiveness of the existing controls. This would inform management of additional control interventions required to better manage the risk exposures to an acceptable level. Management will be able to consider the best control options from various alternative control types.

- **Management controls**

  These ensure that the institutions structure and systems support the policies, plans and objectives and operate within laws and regulations;

- **Administrative controls**

  These ensure that policies and objectives are delivered in an efficient and effective manner and that losses are minimised.

- **Accounting controls**

  These ensure that resources allocated are accounted for fully and transparently and are properly documented.

- **Information Technology controls**

  These controls relate to IT systems and include access control, controls of system software programmes, business continuity controls and other controls.

Each control type above can be classified as either:

- **Preventative controls**

  These controls are designed to discourage errors or irregularities from occurring e.g. adequate physical security of assets to prevent losses such as theft or damage. If properly enforced, these controls are usually the most effective type of controls;

- **Detective controls**

  These controls are designed to find errors or irregularities after they have occurred e.g. performance of reconciliation procedures to identify errors.

- **Corrective controls**

  These controls usually operate together with detective controls in order to correct identified errors or irregularities.

2.7 Information and Communication

Relevant information, properly and timeously communicated to relevant stakeholders, is essential in order to equip such stakeholders to identify, assess and respond to risks.

This may include implementing a risk management reporting system, incident reporting system and emergency risk warning system.

2.8 Monitoring

Risk management should be regularly monitored – a process that assesses both the presence and functioning of its components and the quality of their performance over time. Monitoring can be done in two ways:

- Through ongoing activities, or
- Separate evaluations

This will ensure that risk management continues to be applied at all levels and across the institution.

2.9 Risk Appetite

The Committee of Sponsoring Organisations of the Treadway Commission (COSO) *Enterprise Risk Management – Risk Appetite Framework*, defines risk appetite as follows -
"The amount of risk, on a broad level, an entity is willing to accept in pursuit of value. It reflects the entity's risk management philosophy, and in turn influences the entity's culture and operating style. … Risk appetite guides resource allocation. … Risk appetite [assists the organization] in aligning the organization, people, and processes in [designing the] infrastructure necessary to effectively respond to and monitor risks".

In terms of National Treasury's Risk Management framework, risk appetite means" *The amount of residual risk that the Institution is willing to accept."*

The institution is willing to accept a risk appetite of all risks with a residual rating above 60.

2.10 Risk Tolerance

Risk tolerance is the undesirable variation of risk levels in relation to the achievement of an objective. This refers to an event where the department has deviated from the normal procedures. Management uses risk tolerance to help stay within risk appetite levels, also not to deviate too much from the set strategic parameters i.e. risk appetite.

When setting risk tolerance levels, management must consider the importance of the related objectives and must align tolerance levels with risk appetite. Benefits of setting risk tolerance – Setting risk tolerance is very important as it assists the institution to make decisions based on

what has been determined to be acceptable risk levels. It also assists in determining risk that could be detrimental to the institution's existence. This helps with setting risk or control indicators and with monitoring.

2.11 Risk severity

Risk Severity (also called Risk Impact) is the **expected harm or adverse effect that may occur due to exposure to the Risk**. In other words, it measures how bad things could get if a particular risk materializes.

2.12 Risk rating scales

Rating on Impact

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

"Impact can be defined as the material loss to the organisation, should that risk materialise."

Rating on Likelihood (probability)

The assessment of the likelihood of occurrence of a specific risk evaluates the probability of a specific risk occurring.

The likelihood of occurrence assesses the inherent likelihood of the event occurring in the absence of any processes, which the business may have in place to reduce that likelihood.

3. DRIVERS OF RISK MANAGEMENT

3.1 Risk management as a service delivery imperative

Risk management benefits the institution by underpinning and bolstering institutional performance through:

- More efficient, reliable and cost effective delivery of services
- More reliable decisions
- Innovation
- Minimised waste and fraud
- Better value for money through more efficient use of resources

- Improved project and programme management, which provide better outputs and outcomes.

3.2 Legal Framework

Municipal Entity:

- The Municipal Finance Management Act (Act 56 of 2003)(MFMA);
- Municipal Structures Act (Act 117 of 1998); and
- Municipal Systems Act (Act 32 of 2000).

3.3 Accounting Officer

3.3.1 Section 62(1)(c)(i) of the Municipal Finance Management Act (Act 56 of 2003)(MFMA)

Section 62(1)(c)(i of the MFMA requires that;

"The accounting officer of a municipality is responsible for managing the financial administration of the municipality, and must for this purpose take all responsible steps to ensure-

© that the municipality has and maintains effective, efficient and transparent systems-

- *(i) of financial and risk management and internal control"*

3.4 Management, Other Personnel, Chief Risk Officer, Risk Champions

3.4.1 Section 78 of the Municipal Finance Management Act (Act 56 of 2003) (MFMA)

The extension of general responsibilities in terms of Section 78 of the MFMA to other officials of the municipality implies that responsibility for risk management vests at all levels of management and that it is not limited to only the accounting officer and internal audit.

3.5 Internal Auditors

3.5.1 Section 165(2) (a),(b)(iv) of the Municipal Finance Management Act (Act 56 of 2003) (MFMA)

Section 165(2)(a), (b)(iv) of the MFMA requires that:

"(2) The internal audit unit of a municipality 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 committee on the implementation on the internal audit plan and matters relating to;

- *(iv) risk and risk management"*

3.5.2 Section 2110 – Risk Management of the International standards for the Professional Practice of Internal Auditing

Section 2110 – Risk Management of the International standards for the Professional Practice of Internal Auditing states:

"The internal audit activity should assist the organisation by identifying and evaluating significant exposures to risk and contributing to the improvements of risk management and control systems

2110 A1 – The internal audit activity should monitor and evaluate the effectiveness of the organisation's risk management system

2001 A2 – The internal audit activity should evaluate risk exposures relating to the organisation's governance, operations, and information systems regarding the;

- *Reliability and integrity of financial and operational information;*
- *Effectiveness and efficiency of operations;*
- *Safeguarding of assets;*
- *Compliance with laws, regulations, and contracts*

2110 C1 – During consulting engagements, internal auditors should address risk consistent with the engagement's objectives and be alert to the existence of other significant risks.

2110 C2 – Internal Auditors should incorporate knowledge of risks gained from consulting engagements into the process of identifying and evaluating significant risk exposures of the organisation."

3.6 Audit Committee

3.6.1 Section 166(2)(a)(ii) of the Municipal Finance Management Act (Act 56 of 2003) (MFMA)

Section 166(2)(a)(ii) of the MFMA states:

"(2) An 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"*

3.7 Corporate governance guidelines

Municipalities are encouraged to adhere to the principles espoused in the King IV Report on corporate Governance (King IV) given its promotion of an advanced level of institutional conduct. King IV discusses the following risk management principles, which could be of value to the institution:

- Introduction and definition of risk management;
- Responsibility for risk management;
- Assimilating risk to the control environment; and
- Application of risk management.

Similarly, the principles of Batho Pele clearly articulate the need for prudent risk management to underpin government objectives. Batho Pele strives to instil a culture of accountability and caring by public servants. Further objectives of Batho Pele include supporting the government's governance responsibilities, improving results through more informed decision-making, strengthening accountability and enhancing stewardship and transparency, all of which resonate well with the principles of risk management.

4. ENABLERS OF RISK MANAGEMENT

4.1 Risk Management Strategy

The risk management strategy guides the institution on how to implement its risk management policy.

The strategy should articulate a high level plan of action to improve the institutions risk profile. A Risk Management Implementation Plan informed by the institutions most recent risk profile should supplement the risk management strategy.

4.1.1 Developing a risk management strategy

There is one main output from this particular task. It is a document that describes how ongoing risk management will work in the institution.

The risk management strategy should consider the following five main elements:

- **Structural configuration**

  This element describes how the institution will be structured in terms of committees and reporting lines to give effect to the risk management policy

- **Accountability, roles and responsibilities**

  This element describes the authority and delegation of responsibilities to give effect to the risk management policy.

- **Risk management activities**

  This element includes the risk assessment of whether or not key milestones are achieved. More importantly it is also monitoring whether the risk management strategy is producing the sustainable outcomes as originally envisaged.

- **Assurance activities**

  This element considers all assurance providers available to the institution and integration of their scope of responsibility.

The risk management strategy should include a risk management implementation plan, in the form of a project plan and record the tasks, names of responsible persons and target dates.

Documenting the risk management implementation plan also overcomes problems with changes in personnel and is a good way of creating risk awareness and promoting a culture of risk management.

4.1.2 Developing a risk management implementation plan

The following steps need to be taken when developing the risk management implementation plan:

- Determine the risk management activities to be performed taking into account the risk profile and related costs versus the benefits

- Resourcing requirements

  This element describes the capacity and competence of personnel and the strategy to address capacity gaps. It also addresses the technology and funding requirements to give effect to the risk management strategy

- Determine the sequence of activities and the target implementation dates

  The competition for management attention and resources requires that the sequence of activities should be founded on the principles of urgency, quick wins and sustainability of implemented risk mitigation strategies

- Assign ownership for and communicate risk management activities

- Agree on frequency and format of reporting

4.1.3 Fraud Risk Management Policy and Strategy

A Fraud Prevention Plan represents an important component of the institution's overall risk management strategy and must be addressed by means of a Fraud Risk Management Policy and Fraud Risk Management Strategy

4.2 Basic requirements for effective ERM implementation

The effectiveness of ERM is strongly correlated with the investment of the required resources and application of specialist expertise. Listed below are the required resources:

- Competent people;
- Information, tools and technology;
- Funding for ERM

These fundamental requirements are discussed in more detail in the paragraphs below.

4.2.1 Competent personnel

ERM is affected by various people, sometimes as members of committees, who perform distinctive roles and undertake specific responsibilities. The fact that all people involved in the ERM process must be competent, willing and have the necessary capacity to perform such roles cannot be overemphasised as the vast majority of ERM failures can be attributed to the failure of people rather than the failure of modality.

4.2.2 Organisational structure

The challenge for the institution is to set up appropriate internal structures and delegate roles and responsibilities in such a way that the individual contributions of all role players in terms of risk management can converge in a systematic and coordinated manner. The organisational structure must facilitate efficient reporting relationships and flow of information between these parties.

4.2.3 Role players and responsibilities

ERM is most effective when performance expectations are clearly defined, communicated and integrated into performance agreements, and the responsible persons perform to these expectations.

The people responsible for ERM can be categorised into three distinct categories, namely implementers, support and oversight.

5. IMPLEMENTORS

5.1 Accounting Authority / Officer

The Accounting Authority / Officer are ultimately responsible for risk management within the institution. The Accounting Authority / Officer approve the risk management policy and strategy for the institution and provide leadership and guidance for their implementation. The Accounting Authority / Officer are accountable to the Executive Authority regarding the effectiveness of the risk management process.

5.2 Management

Management owns the risks, thus taking ownership for management of institutional risks.

Management are accountable to the Accounting Authority / Officer to integrate the principles of risk management into their daily routines to enhance the achievement of their service delivery objectives.

5.3 Other personnel

Other personnel are accountable to line management to integrate the principles of risk management into their daily routines to enhance the achievement of their functional objectives.

6. SUPPORT

6.1 Chief Risk Officer (CRO)

The CRO provides specialist expertise in providing a comprehensive support service to ensure systematic, uniform and effective enterprise risk management. The CRO plays a vital communication link between operational level management, senior management, risk management committee and other relevant committees. The CRO is thus the custodian of the ERM framework, the co-ordinator of the risk management throughout the institution and the institutional advisor on all risk management matters.

6.2 Risk Champions

Risk Champions are usually existing members of the senior management corps within the institution. Risk Champions support the risk management process in specific allocated areas or functions.

Risk Champions has sufficient authority to drive ERM as required by the institutions risk management policy and strategy. A key part of the Risk Champions responsibility

involves escalating instances where the risk management efforts are stifled, such as when individuals try to block ERM initiatives.

Risk Champions also adds value to the risk management process by providing guidance and support to manage problematic risks and risks of a transversal nature.

7. OVERSIGHT

7.1 Parliamentary Oversight Structures

Parliamentary Oversight Structures are responsible for overseeing the complete spectrum of governance within an institution. This responsibility would therefore also include an interest in the effectiveness of the process of risk management within the institution.

7.2 Auditor-General

The auditor-General is responsible for providing an opinion on:

- The reasonability of the financial statements of the institution;
- Compliance with applicable legislation

In addition the Auditor-General is required to highlight weaknesses or deficiencies in the performance reporting of the institution. In providing an opinion on compliance with legislation the Auditor-General will provide independent assurance on the effectiveness of the risk management activities of the institution.

7.3 National & Provincial Treasury

National & provincial Treasury have specific duties in terms of the MFMA to monitor and assess the systems of risk management in municipal Entities, assist with building risk management, capacity in Municipal Entities and to enforce the PFMA (by implementing the specific prescripts there in pertaining to risk management) in Municipal Entities.

7.4 Audit committee

The Audit Committee is responsible for assisting the Accounting Officer in addressing its oversight requirements of risk management and evaluating and monitoring the institution's performance with regards to risk management.

7.5 Risk Management Committee

The Risk Management Committee is responsible for oversight of the quality, integrity and reliability of the institutions risk management processes and risk responses. An important part of the Committees mandate is to provide recommendations to the Accounting Officer to

continuously improve the management of specific risks as well as the overall process of risk management.

7.6 Executive Authority

The Executive Authority is accountable to Council in terms of the achievement of the goals and objectives of the institution. In this context the Executive Authority should take an interest in ERM to the extent necessary to obtain comfort that properly established and functioning systems of risk management are in place to protect the institution.

7.7 Internal Auditors

Internal Auditors are responsible for providing independent assurance on the effectiveness of risk management in the institution. This involves providing assurance that all material risks have been identified and assessed and that control systems implemented to treat such risks are both adequate and effective

8. MONITORING

Monitoring enterprise risk management is a process that assesses the presence and functioning of its components over time. This is accomplished through on-going monitoring activities, separate evaluations or a combination of the two. On-going monitoring occurs in the normal course of management activities. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of on-going monitoring procedures.

9. CONTINUOUS IMPROVEMENT

Risk management, like any business activity should be continuously improved. This means that the institution will always strive to move from its current level of risk maturity to a more mature level of risk maturity. This maturity can include improvements in risk governance, risk identification, risk assessment, risk monitoring and risk optimisation.

10. REVIEW OF RISK POLICY

The Committee shall review the risk policy and recommend to Council for approval any amendments that may be required**.**

11. GLOSSARY OF TERMS

Event - An incident or occurrence from internal or external sources that affects the achievement of Beaufort West Municipality's objectives.

Impact - A result or effect of an event. The impact of an event can be positive or negative. A negative event is termed a "risk".

Inherent - The risks to Beaufort West Municipality in the absence of any actions management might take to alter either the risk's impact or likelihood. In other words, the impact that the risk will have on the achievement of objectives if the current controls that are in place, are not considered.

Likelihood / Probability - The probability of the event occurring.

Operations - Used with "objectives", having to do with the effectiveness and efficiency of the municipality's activities, including performance and safeguarding resources against loss.

Priority / Key Risks - Risks that are rated high on an inherent level. Risks that need to be acted upon. Risks that possess a serious threat to the municipality.

Project Risks - Risks that are identified for all major projects, covering the whole lifecycle and include long-term projects.

Reputational Risk - A type of risk related to the trustworthiness of an entity. Damage to the entity's reputation can result in lost revenue or destruction of shareholder value, even if the entity is not found guilty of a crime. Reputational risk can be a matter of corporate trust, but serves also as a tool in crisis prevention

Residual - The remaining exposure after the mitigating effects of deliberate management interventions to control such exposure. (The remaining risk after management has put in place measures to control the inherent risk).

Risk - An unwanted outcome, actual or potential, to the Municipality's service delivery and other performance objectives, caused by the presence of risk factor(s). Some risk factor(s) also present upside potential, which Management must be aware of and be prepared to exploit. This definition of "risk" also encompasses such opportunities.

Risk Appetite - The amount of residual risk that the Municipality is willing to accept.

Risk Factor - Any threat or event which creates, or has the potential to create a risk.

Risk Owner - The person responsible for managing a particular risk.

Risk Management - A systematic and formalised process to identify, assess, manage and monitor risks.

Risk Profile / Register - Also known as the risk register. The risk profile 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. Also describes the willingness of a municipality to take risks and how those risks will affect the operational strategy of the municipality.

Risk Response - Management develop strategies to reduce or eliminate the threats and events that create risks.

Risk Tolerance - The amount of risk the Municipality is capable of bearing (as opposed to the amount of risk it is willing to bear).

Stakeholders - Parties that are affected by the municipality, such as the communities in which the municipality operates, employees, suppliers etc.

Strategic – used with "objectives", it has to do with high-level goals that are aligned with and support the municipality's mission or vision.

Mitigation / Treatment - After comparing the risk score (severity rating = impact X likelihood) with the risk tolerance, risks with unacceptable levels of risk will require treatment plans (additional action to be taken by management and/or Council)