BERGRIVIER MUNICIPALITY

ENTERPRISE RISK MANAGEMENT POLICY

APRIL 2018

HISTORY OF REVIEW AND APPROVAL

Author of Document:

Version	Author	Date Compiled
1.0	Chief Risk Officer: Madell Lihou	April 2013
		Based on policy as developed by Corporate Governance, Provincial Treasury.
1.1	Chief Risk Officer: Madell Lihou	September 2014
1.2	Chief Risk Officer: Madell Lihou	November 2015
1.3	Jurene Erasmus	November 2016
1.4	Jurene Erasmus	November 2017

Reviewed and Recommended By:

Version	Reviewed By	Comments	Date Reviewed
1.0	Risk Management Committee	Recommended with minimal changes to be made by CRO.	7 May and 20 September 2012.
1.1	Risk Management Committee	Recommended with minimal changes	17 September 2014
1.2	Risk Management	Recommended with minimal changes	03 December 2015
1.3	Risk Management Committee	Recommended with minimal changes	01 December 2016
1.4	Risk Management Committee	Recommended with no changes	30 November 2017

Approved By:

Version	Approval By	Date Approved
1.0	Council (Resolution No. …..)	May 2013
1.1	Council (Resolution No. …..)	March 2015
1.2	Council (Resolution No.RVN10/05/2016)	May 2016
1.4	Mayco (Resolution No BKN039/06/2017)	June 2017
1.3	Mayco (Resolution No BKN037/04/2018)	April 2018

RISK MANAGEMENT PHILOSOPHY

Bergrivier Municipality is committed to the optimal management of risk in order to protect our core public service values, achieve our vision, objectives and deliver on our core business.

In the course of conducting our day-to-day business operations, we are exposed to a variety of risks. These risks include operational and other risks that are material and require comprehensive controls and on-going oversight.

To ensure business success we have adopted an enterprise-wide integrated approach to the management of risks. By embedding the risk management process into key business processes such as planning, operations and new projects, we will be better equipped to identify events affecting our objectives and to manage risks in ways that are consistent with the approved risk appetite.

To further implement this approach, all roles players involved in the risk management process were identified and their responsibilities clearly documented to enforce a culture of disciplined risk-taking.

Council is responsible for the overall governance of risk within the municipality. Council has however delegated this responsibility to the Municipal Manager (MM) and the risk management oversight committee. The MM, who is ultimately responsible for the municipality's risks, has delegated this role to the Chief Risk Officer (CRO)and Management. The CRO will ensure that the framework is implemented and that council, the RMC, the Audit Committee and the MM receive appropriate reporting on the municipality's risk profile and risk management process. Management will execute their responsibilities outlined in the Risk Management Strategy and Implementation Plan. All other officials are responsible for incorporating risk management into their day-to-day operations.

As the MM of the municipality, council and I are responsible for enhancing corporate governance. Entrenching Enterprise Risk Management (ERM) into the municipality is only but one component of governance, but together we will ensure that appropriate focus is placed on important tasks and key risks.

SIGNATURE OF MUNICIPAL MANAGER:

_____

ADV HANLIE LINDE
DATE:

1. OVERVIEW

1.1. Policy Objective

The objective of this policy is to safeguard Bergrivier Municipality's property, interests and safeguard people.

1.2. Policy Statement

Through this policy, the MM puts into practice the municipality's commitment to implement and maintain an effective, efficient and transparent system of risk management. This policy forms the basis for the accompanying Risk Management Strategy and Implementation Plan which is designed to help achieve the objective of implementing an effective ERM process and embedding a culture of risk management within the municipality.

1.3. Policy Scope

This is an enterprise-wide policy. It applies throughout Bergrivier Municipality in as far as risk management is concerned as all personal within the municipality has a role to play in the identification and management of risk.

1.4. Background

1.4.1. Legislative Mandate

Section 62(1)(c)(i) and 95(c)(i)of the MFMA states that: "… The accounting officer of the municipality and municipal entity is responsible for managing the financial administration of the municipality, and must for this purpose take all reasonable steps to ensure that the municipality has and maintains effective, efficient and transparent systems of financial and risk management and internal control."

1.4.2. Legislative Compliance

This policy is aligned to the principles set out in the National Treasury Public Sector Risk Management Framework, published on 1 April 2010 and to some extent King III. This policy is also supported by the MFMA, Act no. 56 of 2003.

1.4.3. Objectives of Enterprise Risk Management

The objective of risk management is to assist management in making more informed decisions which:

- provide a level of assurance that current significant risks are effectively managed;
- improve operational performance by assisting and improving decision making and planning;
- promote a more innovative, less risk averse culture in which the taking of calculated risks in pursuit of opportunities, to benefit the municipality is encouraged; and
- provide a sound basis for integrated risk management and internal control as components of good corporate governance.

1.4.4. Benefits of Enterprise Risk Management

The risk management process can make major contributions towards helping the municipality achieve its objectives. The benefits include:

- more sustainable and reliable delivery of services;
- enhance decision making underpinned by appropriate rigour and analysis;
- reduced waste;
- prevention of fraud and corruption;
- fewer surprises and crises by placing management in a position to effectively deal with potential new and emerging risks that may create uncertainty;
- help avoid damage to the municipality's reputation and image;
- helps ensure effective reporting and compliance with laws and regulations;
- better value for money through more effective, efficient and economical use of scarce resources; and
- better outputs and outcomes through improved project and programme management.

1.5. Key Concepts

1.5.1. Risk is an uncertain future event that could influence the achievement of the municipality's strategic and business objectives.

1.5.2. Risk Management is a systematic and formalised process instituted by the municipality to identify, assess, manage, monitor and report risks to ensure the achievement of objectives.

1.5.3. Enterprise Risk Management (ERM) is the application of risk management throughout the municipality rather than only in selected business areas or disciplines and needs to be managed in a comprehensive and integrated way. ERM recognises that risks (including

opportunities) are dynamic, often highly interdependent and ought not to be considered and managed in isolation.

2. ENTERPRISE RISK MANAGEMENT PROCESS

To fulfil its philosophy and implement an enterprise-wide integrated approach Bergrivier Municipality will ensure that the eight (8) components of the ERM process are implemented and operating effectively, efficiently and economically***(Refer to figure 1)***. These components of the ERM process are discussed in further detail in the Risk Management Strategy and implementation plan.

Figure 1: Enterprise Risk Management Process

2.1. Internal Environment

The municipality's internal environment is the foundation of all other components of risk management. The internal environment encompasses the tone of Bergrivier Municipality, influencing the risk consciousness of its people. It is the foundation for all other components of risk management, providing discipline and structure.

2.2. Objective Setting

Objective setting is a precondition to event identification, risk assessment, and risk response. There must first be objectives before management can identify risks to their achievement and take necessary actions to manage the risks.

2.3. Event Identification

An event is an incident or occurrence emanating from internal or external sources that could affect implementation of strategy or achievement of objectives. Events may have positive or negative impacts, or both. As part of event identification, management recognises that uncertainties exist, but does not know when an event may occur, or its outcome should it

occur. To avoid overlooking relevant events, identification is best made apart from the assessment of the likelihood of the event occurring, which is the topic of risk assessment.

2.4. Risk Assessment

Risk assessments allow the municipality to consider the extent to which potential events might have an impact on the achievement of objectives. Management assess events from two perspectives impact and likelihood to determine their risk score or severity rating and normally uses the quantitative method.

Risk Assessments are performed through a three stage process:

- Firstly, inherent risk should be assessed;
- Secondly, residual risk should be assessed;
- Thirdly, the residual risk should be benchmarked against the risk appetite to determine the need for further intervention.

This is done as per the Risk assessment methodology document.

2.4.1. Risk Appetite

Risk appetite looks at how much risk a municipality is willing to accept. The aim is to manage risks by taking action to keep exposure to an acceptable level in cost-effective way. There can still be deviations that are within a risk appetite as every control has an associated cost. The control action must offer value for money in relation to the risk that it is controlling. Although the risk is within the risk appetite, management can still implement more controls to bring the level down if it is cost effective.

Bergrivier Municipality has set its risk appetite level at Impact x Likelihood = 4x10 & 10x4 (40/100).

The municipality has committed itself to aggressively pursue managing risks to be within its risk appetite to avoid exposures to losses and to manage actions that could have a negative impact on the reputation of the municipality.


Severity
Likelihood
Higher
Lower
More
Less
Unacceptable
Acceptable with Mitigation
Acceptable

2.5. Risk Response

After assessing the risk scores an appropriate mitigation strategy is selected. These responses may fall within the categories of avoid, reduce, share and accept. *(Refer to figure 3*).

Risk responses fall within the following four categories:

- **Avoid –** Action is taken to exit the activities giving rise to risk. Risk avoidance may involve exiting a product line, declining expansion to a new geographical market, or selling a division.
- **Reduce –** Action is taken to reduce the risk likelihood or impact, or both. This may involve any of a myriad of everyday business decisions.
- **Share –**Action is taken to reduce risk likelihood or impact by transferring or otherwise sharing a portion of the risk. Common risk sharing techniques include purchasing insurance products, pooling risks, engaging in hedging transactions, or outsourcing an activity.
- **Accept –**No action is taken to affect likelihood or impact.

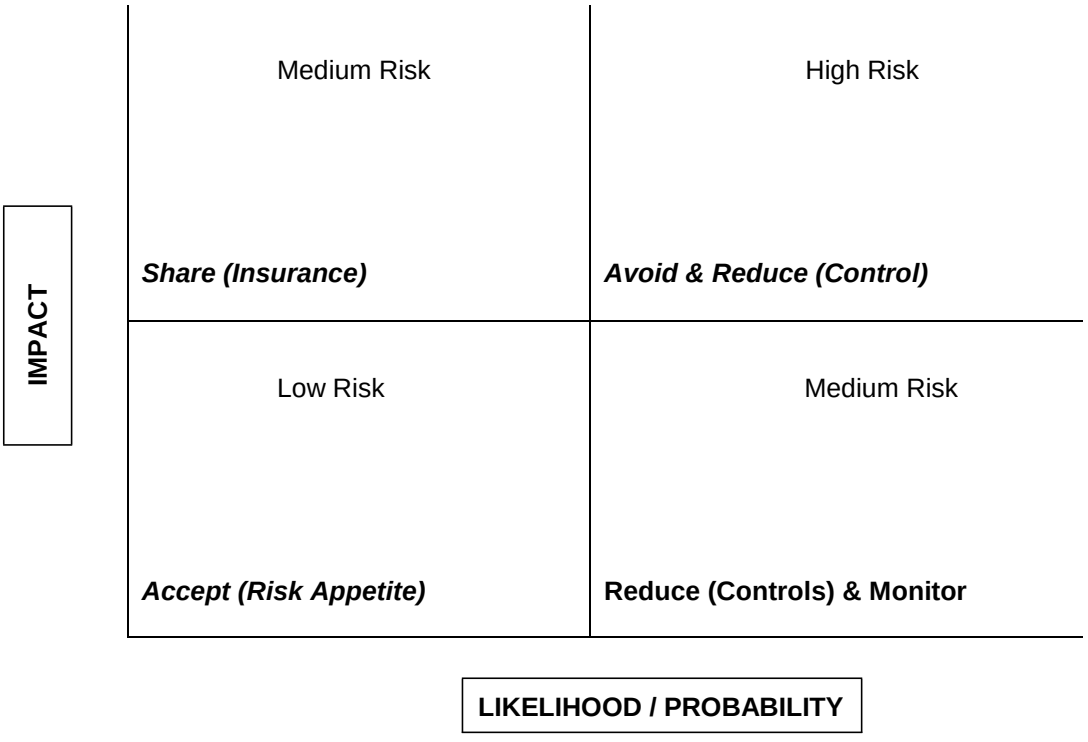

Figure 3: Risk Response Strategy

2.6. Control Activities

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.

Types of Control Activities

Many different descriptions of types of control activities have been put forth. Internal Controls can be preventative, detective or corrective by nature.

- Preventative Controls are designed to keep errors or irregularities from occurring in the first place.
- Detective Controls are designed to detect errors or irregularities that may have occurred.
- Corrective Controls are designed to correct errors or irregularities that have been detected.

2.7. Information and Communication

Pertinent information is identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs, flowing down, across and up in the municipality. All personnel receive a clear message from top management that risk management responsibilities must be taken seriously. They understand their own role in risk management, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There is also effective communication with external parties.

2.8. Monitoring

Monitoring 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.

3. ROLES AND RESPONSIBILITIES (COSO THREE LINES OF DEFENCE MODEL)

The Three Lines of Defense (3 LOD) addresses how specific duties related to risk and control are assigned and coordinated within the municipality, regardless of its size or complexity. Directors and Management should understand the critical differences in roles and responsibilities of these duties and how they should be optimally assigned for the municipality to have increases likelihood of achieving its objectives.

The following figure shows the relationship among objectives, the framework and the model:

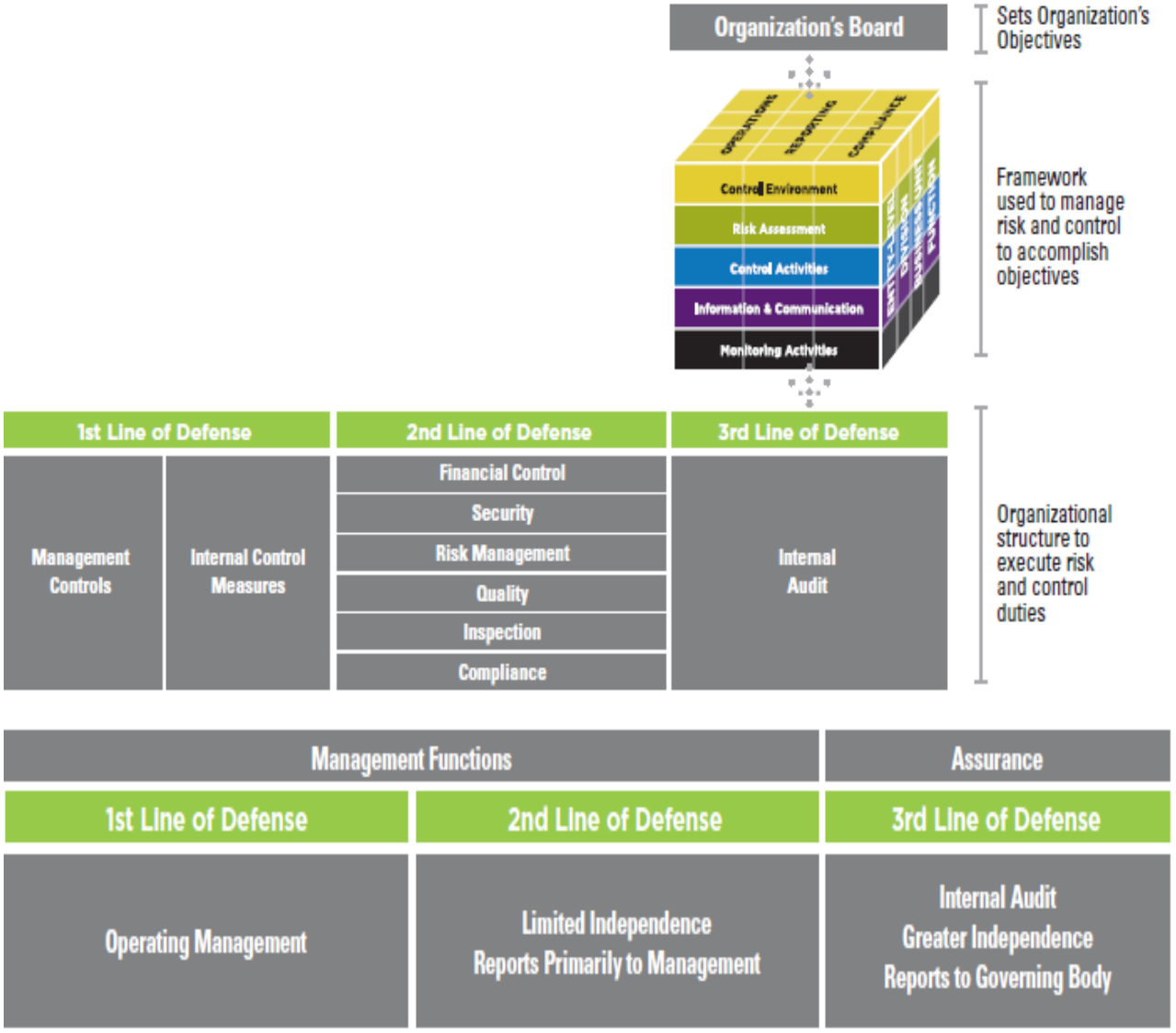

Figure 1: Differences between the three lines of defense.

3.1. Risk Management Oversight

Senior Management, Council and the Performance, Risk and Financial Audit Committee (AC) have integral roles in three Lines of Defense (3 LOD).

3.1.1. Council and Senior Management

Senior Management is accountable for the selection, development and evaluation of the system of internal control with oversight by the Council and Audit Committee. Although neither Senior Management nor the Council is considered to be part of one of the three lines, these parties collectively have responsibility for establishing an Organisation`s objectives, defining high – level strategies to achieve those objectives, and establishing governance structures to best manage risk.

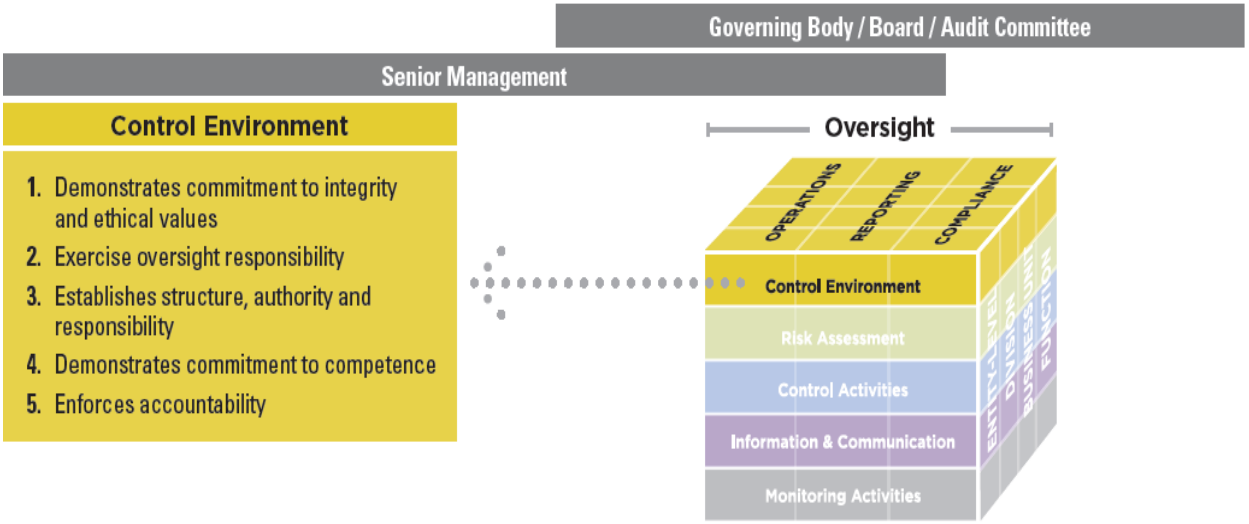

Figure 2: Oversight responsibility for the Control Environment

Council is responsible for the governance of risk. Council takes an interest in risk management to the extent necessary to obtain comfort that properly established and functioning systems of risk management are in place to protect Bergrivier Municipality against significant risks.

Council has to report to the community, on the municipality's system of internal control. This provides comfort that the municipality is protected against significant risks to ensure the achievement of objectives as detailed in the Service Delivery and Budget Improvement Plan (SDBIP).

Council ***must*** perform the following tasks, to fulfil its mandate with regard to ERM.

Ref.	Activity	Frequency
01	Understand, determine and approve the risk appetite with guidance from the CRO and the RMC.	Annually
02	Ensure that frameworks and methodologies are developed and implemented.	Annually
03	Ensure that IT, fraud& corruption and Occupational Health and Safety (OHS) risks are considered as part of the municipality's risk management activities.	Annually
04	Ensure that risk assessments (strategic and operational) are performed by reviewing the RMC reports.	Annually
05	Ensure that assurance regarding the effectiveness of the ERM process is received from the MM, RMC and the Audit Committee	Annually
06	Disclose how they have satisfied them self that risk assessments, responses and interventions are effective as well as undue, unexpected or unusual risks and any material losses (the annual report to include a risk disclosure).	Annually
07	Ensure that management implements, monitors and evaluates performance through the RMC reports.	Annually

3.1.2 Municipal Manager

The MM is ultimately responsible for risk management within the municipality. This includes ensuring that the responsibility for risk management vests at all levels of management. The MM sets the tone at the top by promoting accountability, integrity and other factors that will create a positive control environment.

The MM ***must*** perform the following tasks, to fulfil its mandate with regard to ERM.

Ref.	Activity	Frequency
32	Understand and determine the risk appetite with guidance from the CRO and the RMC.	Annually
33	Ensure that frameworks and methodologies are developed and implemented.	Annually
34	Appoint adequate staff capacity to drive the ERM activity.	As the need arises
35	Appoint a RMC with the necessary skills, competencies and attributes.	As the need arises
36	Ensure that the control environment supports the effective functioning of ERM.	Quarterly
37	Hold officials accountable for their specific risk management responsibilities.	Ongoing
38	Devote personal attention to overseeing management of significant risks.	Quarterly

Ref.	Activity	Frequency
39	Ensure appropriate action in respect of recommendations of the AC, Internal Audit, External Audit and RMC to improve ERM.	Quarterly
40	Evaluate the value add of risk management. (NT financial management maturity capability model)	Annually
41	Provide assurance to relevant stakeholders that key risks are properly identified, assessed and mitigated.	Quarterly
42	Provide leadership and guidance.	Ongoing

3.1.3 Management

All other levels of management, support the municipality's risk management philosophy, promote compliance with the risk appetite and manage risks within their areas of responsibility.

Management takes ownership for managing the municipality's risks within their areas of responsibility and is accountable to the MM for designing, implementing, monitoring an integrating ERM into their day-to-day activities of the municipality. This should be done in a manner that ensures that risk management becomes a valuable strategic management tool.

Management ***must*** perform the following tasks, to fulfil its mandate with regard to ERM.

Ref.	Activity	Frequency
43	Execute their responsibilities as set out in the approved Risk Management Strategy.	Daily
44	Report to the RMC regarding the performance of internal controls for those risks in the operational risk registers.	Quarterly
45	Devote personal attention to overseeing the management of key risks within their area of responsibility.	Ongoing
46	Empower officials to perform effectively in their risk management responsibilities.	Ongoing
47	Maintain a co-operative relationship with the CRO and Risk Champions.	Ongoing
48	Maintain the proper functioning of the control environment within their area of responsibility.	Ongoing
49	Hold officials accountable for their specific risk management responsibilities.	Ongoing
50	Continuously monitor the implementation of risk management within their area of responsibility.	Ongoing

3.2. Performance and Audit Committee (PAC)

The PAC is an independent committee, responsible for oversight of the municipality's control, governance and risk management. This committee is vital to, among other things, ensure that financial, IT and fraud risk related to financial reporting are identified and managed.

The PAC's primary responsibility is providing an independent and objective view of the effectiveness of the municipality's risk management process to Council and to provide recommendations to the MM for continuous improvement and management of risks. The responsibilities of the PAC with regard to risk management are formally defined in its charter.

The Performance and Audit Committee must perform the following tasks, to fulfil its mandate with regard to ERM.

Ref.	Activity	Frequency
08	Formally define its responsibility with respect to risk management in its charter.	Annually
09	Ensure that combined assurance is given to address all the significant risks facing the municipality.	Annually
10	Advice council on risk management. (This will be clearly defined in the charter)	Annually
11	Review the internal and external audit plans and ensure that these plans address the risk areas of the municipality.	Annually
12	Review and recommend disclosures on matters of risk and risk management in the Annual Financial Statements (AFS).	Annually
13	Include statements regarding risk management performance in the annual report to stakeholders.	Annually
14	Evaluate the effectiveness of Internal Audit in its responsibilities for risk management.	Annually
15	Provide regular feedback to the MM on the adequacy and effectiveness of risk management in the municipality.	Quarterly

Ref.	Activity	Frequency
16	Ensure that internal and external audit plans are aligned to the risk profile of the municipality.	Annually
17	Ensure that all risk including, IT, fraud & corruption and OHS risks have been properly addressed.	Quarterly
18	Provide an independent and objective view of the municipality's risk management effectiveness.	Annually

3.2.1. Risk Management Committee (RMC)

The committee's 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.

The RMC ***must*** perform the following tasks, to fulfil its mandate with regard to ERM.

Ref.	Activity	Frequency
19	Formally define its roles and responsibilities with respect to risk management in its charter.	Annually
20	Review and recommend approval of the Risk Management Policy to the MM.	Annually
21	Review and recommend approval of the Risk Management Strategy to the MM.	Annually
22	Provide guidance to the MM, CRO and other relevant risk management stakeholders on how to manage risks to an acceptable level.	Quarterly
23	Provide timely and useful reports to the MM on the state of ERM, together with recommendations.	Quarterly
24	Share risk information with the Audit Committee.	Quarterly
25	Evaluate the extent and effectiveness of integration of ERM within The municipality.	Quarterly
26	Assess implementation of the Risk Management Policy and Strategy.	Quarterly
27	Review material findings and recommendations by assurance providers on the system of risk management and monitor implementation of such recommendations.	Quarterly
28	Develop KPIs for the MMs approval.	Annually
29	Measure and understand the municipality's overall exposure to fraud And corruption and ensure that proper processes are in place to prevent these risks from materializing.	Quarterly
30	Measure and understand the municipality's overall exposure to IT And ensure that proper processes are in place to prevent these risks from materializing.	Quarterly

Ref.	Activity	Frequency
31	Measure and understand the municipality's overall exposure to Occupational Health & Safety (OH&S) and ensure that proper processes are in place to prevent these risks from materialising.	Quarterly

3.3 RISK MANAGEMENT IMPLEMENTERS

3.3.1 OPERATIONAL MANAGEMENT – FIRST LINE OF DEFENCE

The first line of defines is primarily handled by front – line and mid – line managers who have day to day ownership and management of risk and control. Operational Management develop and implement the Organisation`s control and risk management processes. These include internal control processes designed to identify and assess significant risks, execute activities as intended, highlight inadequate processes, address control breakdowns, and communicate to key stakeholders of the activity.

Senior Management takes ownership for managing the municipality's risks within their areas of responsibility and is accountable to the MM for designing, implementing, monitoring and integrating ERM into their day-to-day activities of the municipality.

This should be done in a manner that ensures that risk management becomes a valuable strategic management tool by ensuring that risks are identified upfront and adequate controls are implemented to mitigate these risks. Senior Management has overall responsibility for all first line activities. For certain high risk areas, senior management may also provide direct oversight of the front – line and mid – line management, even to the extent of performing some of the first line responsibilities themselves.

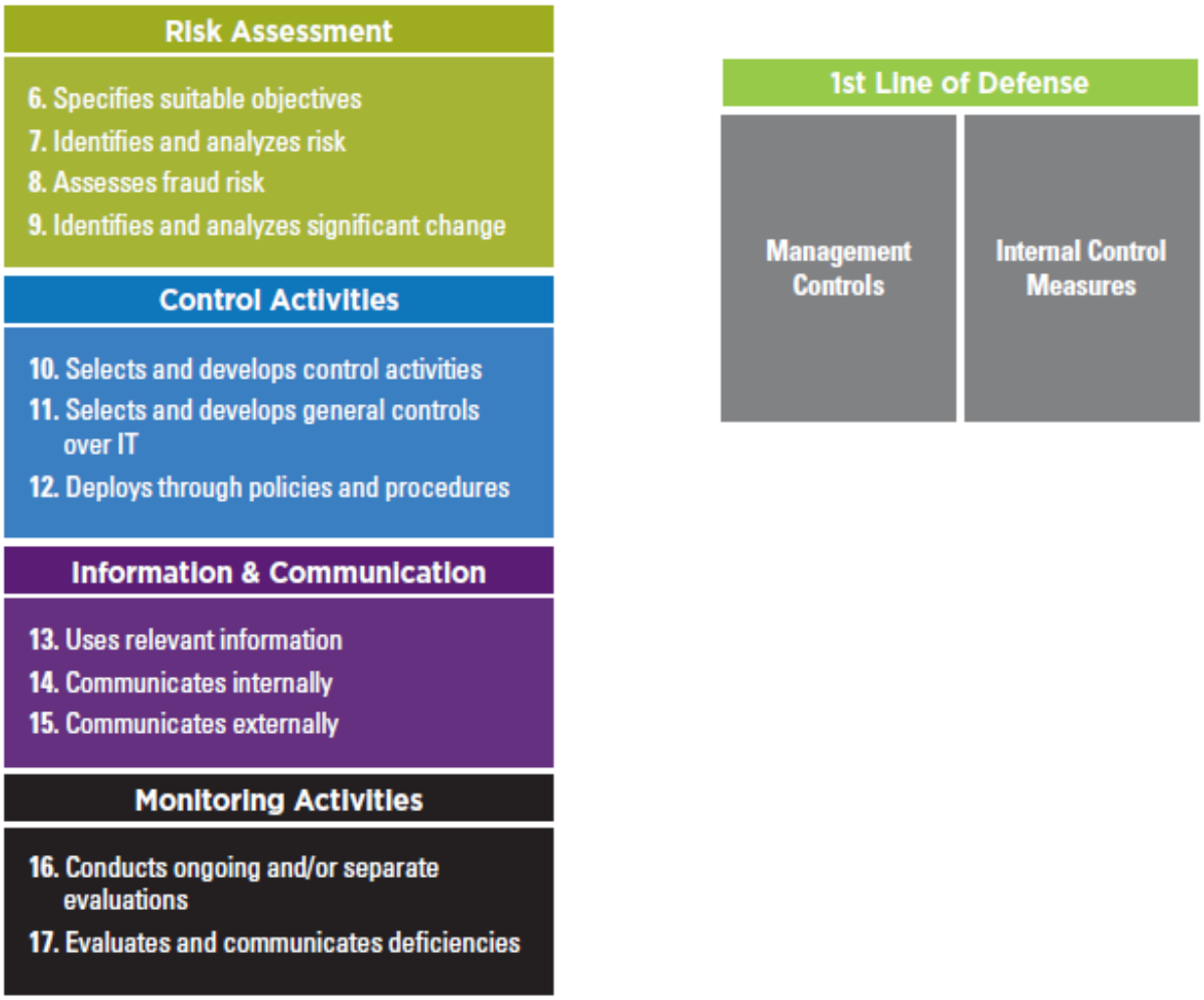

Figure 3: COSO and the 1st Line of Defense

3.2.3. Other Officials

Other officials are responsible for integrating risk management into their day-to-day activities i.e. by ensuring conformance with controls and compliance to procedures.

Other officials ***must*** perform the following tasks, to fulfil its mandate with regard to ERM.

Ref.	Activity	Frequency
51	Take the time to read and understand the content in the Risk Management Policy, but more importantly understanding their roles and responsibilities in the risk management process.	Constantly
52	Apply the risk management process in their respective functions.	Ongoing
53	Inform their supervisors and/or the risk management unit (CRO) Of new risks and significant changes.	As the need arises
54	Co-operate with other roles players in the risk management process.	Ongoing
55	Provide information to role players in the risk management process as required.	As the need arises

3.4.1 RISK MANAGEMENT – SECOND LINE OF DEFENCE

The second line of defence includes various risk management and compliance functions put in place by management to help ensure controls and risk management processes implemented by the first line of defence are designed appropriately and operating as intended.

These are management function; separate from first – line operating management, but still under the control and direction of senior management. Functions in the second line of defence are typically responsible for ongoing monitoring of control and risk. They often work closely with operating management to help define implementation strategy, provide expertise in risk, implement policies and procedures, and collect information to create an enterprise-wide view of risk and control.

The responsibilities of individuals within the second line of defines vary widely but typically include:

- Assisting management in design and development of processes and controls to manage risks.
- Defining activities to monitor and how to measure success as compared to management expectations.
- Monitoring the adequacy and effectiveness of internal control activities.
- Escalating critical issues, emerging risks and outliers
- Providing risk management frameworks.
- Identifying and monitoring known and emerging issues affecting the organization's risks and controls.
- Identifying shifts in the organization's implicit risk appetite and risk tolerance.
- Providing guidance and training related

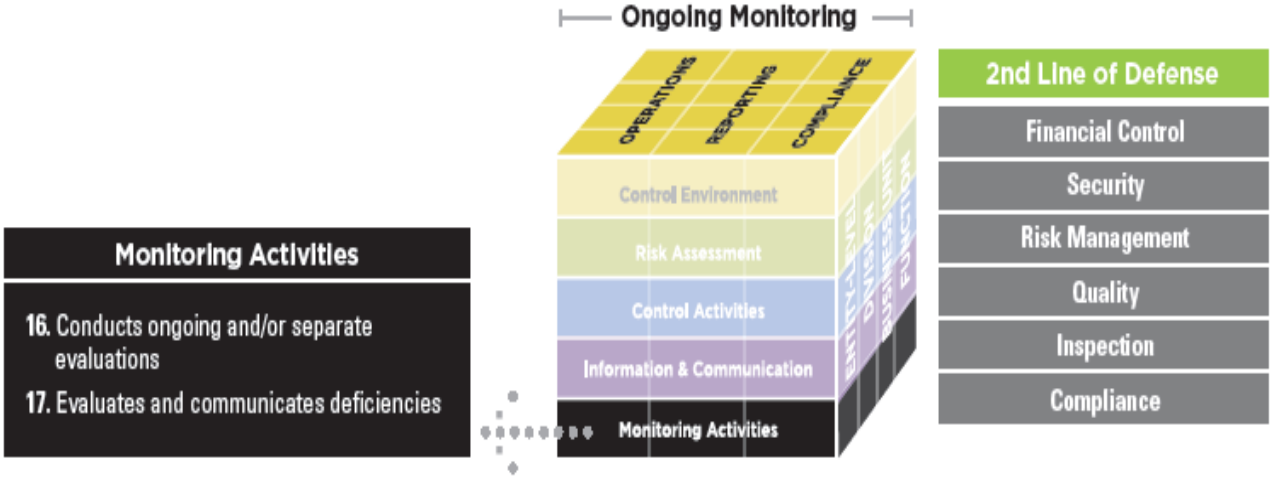

Figure 4: COSO and the 2nd Line of Defense.

Typical second-line functions include specialty expertise groups such as:

- Information Security
- Health and Safety
- Legal
- Environmental
- Supply chain

3.4.2. Risk Management Support

3.4.2.1 Chief Risk Officer

The CRO (Internal Auditor) is the custodian of the Risk Management Strategy and Implementation Plan and the coordinator of ERM activities throughout Bergrivier Municipality. The primary responsibility of the CRO is to use her specialist expertise to assist the municipality to embed ERM and leverage its benefits to enhance performance. The CRO plays a vital communication link between senior management, operational level management, the RMC and other relevant committees.

The CRO ***must*** perform the following task, to fulfil its mandate with regard to ERM.

Ref.	Activity	Frequency
56	Assist the MM and senior management develop the municipality's vision for risk management. (Philosophy)	Annually
57	Develop, in consultation with management, the municipality's risk management framework and methodologies.	Annually
58	Research and develop the risk rating scales.	Annually
59	Communicate the municipality's risk management framework and methodologies to all stakeholders.	Annually
60	Facilitate orientation and training for RMC.	As the need arises
61	Train all stakeholders in their ERM responsibilities.	Quarterly
62	Continuously drive ERM to higher levels of maturity.	Ongoing
63	Coordinate and facilitate the assessments.	Quarterly
64	Prepare ERM registers, reports and dashboards for submission to the RMC and other roles players.	Quarterly
65	Coordinate the implementation of response strategies.	Ongoing
66	Ensure that all IT, fraud, OHS risks are considered as part of the municipality's ERM activities.	Ongoing
67	Avail the approved risk registers to Internal Audit on request.	As the need arises
68	Consolidate risk identified by the various Risk Champions.	Quarterly
69	Participate with Internal Audit, Management and AG in developing the combined assurance plan.	Annually

3.4.2.2. Risk Champions

A Risk Champion would generally hold a senior position within the municipality and possess the skills, knowledge and leadership qualities required to champion a particular aspect of risk management.

The Risk Champion assist the CRO facilitate the risk assessment process and manage risks within their area of responsibility to be within the risk appetite. Their primary responsibilities are advising on, formulating, overseeing and managing all aspects of a municipality's entire risk profile, ensuring that major risks are identified and reported upwards.

Risk Champions ***must*** perform the following tasks, to fulfil its mandate with regard to ERM.

Ref.	Activity	Frequency
70	Facilitate operational risk workshops for their area of responsibility with the assistance of the CRO.	Quarterly
71	Co-ordinate the implementation of action plans for the risk and report on any developments regarding the risk.	Quarterly
72	Populate the risk registers/dashboard.	Ongoing
73	Ensure that all risk information is updated regularly and submitted to the CRO.	Ongoing
74	Provide assurance regarding the risk's controls.	Ongoing

3.4. Risk Management Assurance Providers

The core role of Internal Audit in risk management is to provide an independent, objective assurance to council and the 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*** perform the following tasks, to fulfil its mandate with regard to ERM.

Ref.	Activity	Frequency
75	Provide assurance on the ERM process design and its effectiveness.	Annually
76	Provide assurance on the management of "key risks" including, the Effectiveness of the controls and other responses to the "key risks.	Annually
77	Provide assurance on the assessment and reporting of risk and Controls.	Annually

Ref.	Activity	Frequency
78	Prepare a rolling three (3) year Internal Audit plan based on its assessment of key areas of risk.	Annually

3.5 INTERNAL AUDIT – THIRD LINE OF DEFENCE (Assurance of Risk Management to be outsourced)

Internal Auditors serve as an Organisation`s third line of defence. Among other roles, internal audit provides assurance regarding the efficiency and effectiveness of governance, risk management, and internal control. Internal Auditors do not design or implement controls as part of their normal responsibilities and are not responsible for the Organisation`s operations. Because of this high level of independence, internal auditors are optimally positioned for providing reliable and objective assurance to the Council, AC and Senior Management regarding governance, risk and control.

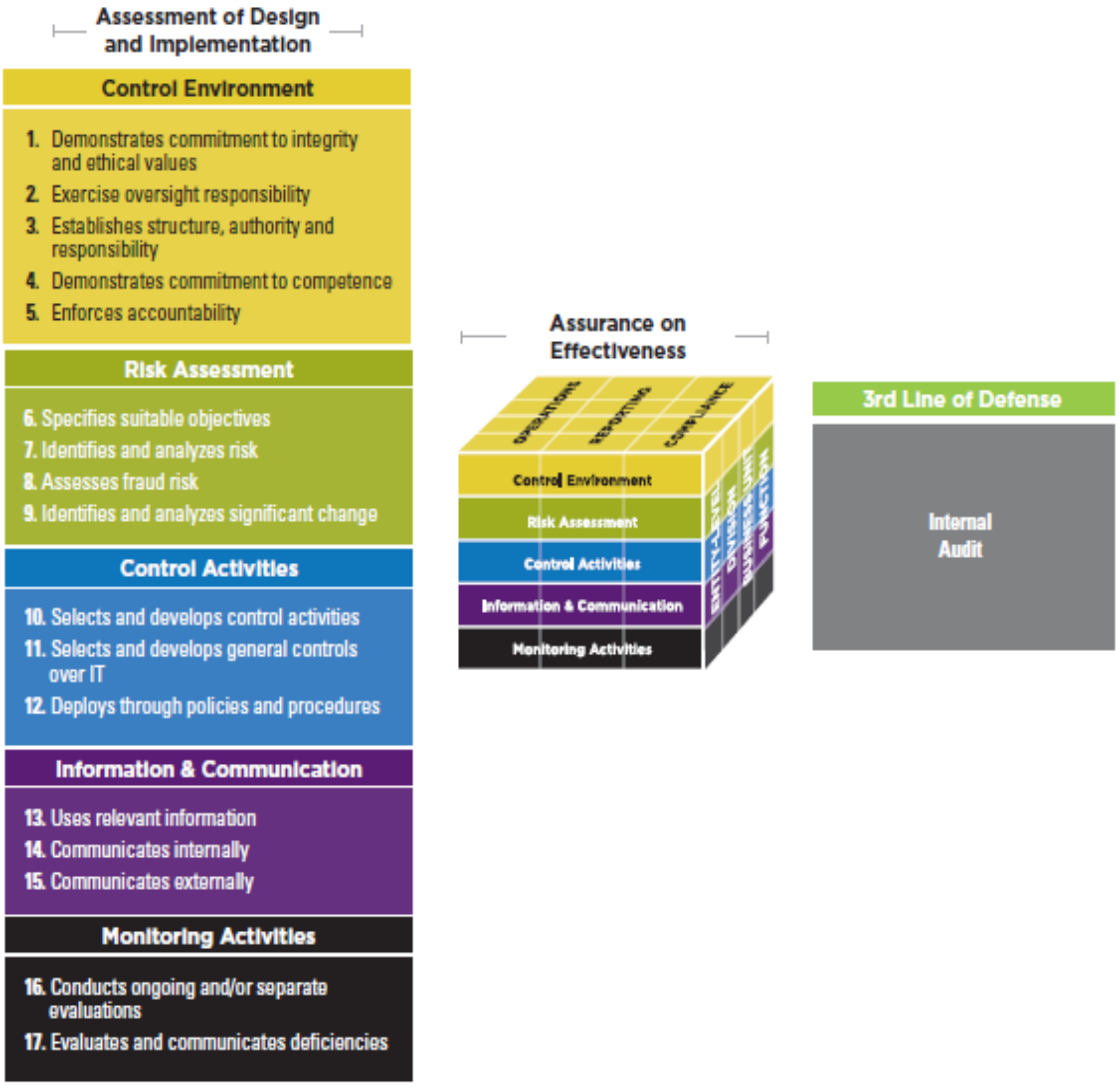

Figure 5: COSO and the 3rd Line of Defense.

3.4.2. External Audit

External Audit (Auditor-General) provides and independent opinion on the effectiveness of ERM.

External Audit ***must*** perform the following tasks, to fulfil its mandate with regard to ERM.

Ref.	Activity	Frequency
79	Determine whether the risk management framework and methodologies are in place and appropriate.	Annually
80	Assess the implementation of the risk management framework and Methodologies.	Annually
81	Review the risk identification process to determine if it is sufficiently To facilitate the timely, correct and complete identification of significant risks.	Annually
82	Review the risk assessment process to determine if it is sufficient to facilitate timely and accurate risk rating and prioritization.	Annually
83	Determine whether management action plans to mitigate the key risks are appropriate and are being effectively implemented.	Annually

4. POLICY REVIEW

The content of the ERM policy will be reviewed annually to reflect the current stance on risk management within the Bergrivier Municipality.

5. GLOSSARY OF TERMS

Accounting Officer refers to the Municipal Manager.

CRO refers to the Chief Risk Officer. In the absence of a CRO the Internal Auditor fulfills this role.

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

Framework *refers* to the National Treasury Public Sector Risk Management Framework, 1 April 2010.

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

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 possess a serious threat to the municipality.

Likelihood / Probability *means* the probability of the event occurring.

Management refer to all levels of management, other than the MM and the CRO.

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)

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 *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 Appetite *means* the amount (level) of risk the municipality is willing to accept.

Risk Owner *means* the person responsible for managing a particular risk.

Risk Management Strategy includes the detailed risk management implementation plan, fraud prevention policy and fraud prevention strategy and implementation plan

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 company to take risks and how those risks will affect the operational strategy of the municipality.

Risk Tolerance *means* the acceptable level of risk that the municipality has the ability to tolerate.

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

6. APPROVAL

Recommended by the Risk Management Committee:

Signature: _____

Name in Print: _____

Date: _____

Position: Chairperson

Approved by the Municipal Manager:

Signature: _____

Name in Print: _____

Date: _____

Position: Municipal Manager

IMPACT RATING SCALE

The impact of occurrence will be assessed as follows:

SCORE	GRADING	FINANCIAL	SERVICE DELIVERY	REPUTATION & IMAGE	EMPLOYEE WELLNES	LEGAL/REGULARITY/ COMPLIANCE
	Descriptions	Impacts of a financial nature and directly affects the institutions budget.	Impacts on the ability to provide maximum services to the stakeholders with existing resources.	Impact is of a reputational nature stemming from bad publicity of the institution.	Impact stems from employees not being in the best mental, emotional and physical state to perform duties.	Impact is on the ability to comply with acts, laws, regulations or contracts as well as with policies and procedures.
10	Catastrophic	Loss of assets, adverse impact on annual revenues. Financial loss of 80 – 100% of budget.	Threatens on-going existence of the component/sub- directorate (Total disruption of service rendered by component/ sub-directorate).	Total loss of confidence within stakeholders. Sustained negative publicity or damage to reputation from a national, sector or community perspective – long term.	Multiple deaths more than 20% unit capacity. Destruction of the institution.	Total shut down of the component or external intervention required
9	Critical	Loss of assets, adverse impact on annual revenues.	Permanent loss of critical information, substantial disruption to component	Critical breakdown in key relationship with primary	Multiple deaths less than 20% unit capacity. Temporary	

SCORE	GRADING	FINANCIAL	SERVICE DELIVERY	REPUTATION & IMAGE	EMPLOYEE WELLNES	LEGAL/REGULARITY/ COMPLIANCE
		Financial loss of 70 – 79% of budget.	or external intervention extending over 6 months or more (Total disruption of service rendered by component/ sub- directorate). Major KRA's not achieved.	stakeholders.	destruction of the institution.	
8	Severe/Major	Loss of assets, adverse impact on annual revenues. Financial loss of 60 – 69% of budget.	Permanent loss of critical information, substantial disruption to component or external intervention extending over 3 to 6 months (Total disruption of service rendered by component/ sub-directorate). All major KRA's not achieved.	Widespread negative reporting in media. Leads to a high-level independent investigation with adverse findings. Short term breakdown in key relationship with stakeholders.	Death. Entrenched morale problems. Inability to recruit employees with necessary skills. Employee walkout.	
7	Significant	Loss of assets, adverse impact on annual revenues.	Considerable remedial effort required with widespread disruption to the component extending for period up to 3 months	Short term breakdown in key relationship with stakeholders. Widespread negative reporting in media.	Serious permanent injury – inability to return to work. On- going widespread morale issues. Extreme	Serious failure to comply with legal or regulatory requirements that may result in legal action

SCORE	GRADING	FINANCIAL	SERVICE DELIVERY	REPUTATION & IMAGE	EMPLOYEE WELLNES	LEGAL/REGULARITY/ COMPLIANCE
		Financial loss of 50 – 59% of budget.	More than 50% of major KRA's will not be achieved.	Premier or Ministerial involvement. Leads to a preliminary investigation with limited findings.	employee turnover.	taken against the institution due to non-compliance with laws, acts, regulations or contracts.
6	Moderate	Loss of assets, adverse impact on annual revenues. Financial loss of 40 – 49 % of budget.	Considerable remedial effort required with limited disruption to the component extending for period 3 months or more Less than 50% of major KRA's will not be achieved.	Limited breakdown in key relationship with stakeholders. Widespread negative reporting in media. Premier or Ministerial involvement.	Serious permanent injury but able to return to work. On-going widespread morale issues. High employee turnover.	
5	Marginal	Loss of assets, adverse impact on annual revenues. Financial loss of 30 – 39% of budget.	Considerable remedial effort required with limited disruption to the component extending for period of less than 3 months. Some KRA's will not be achieved.	Widespread negative reporting in media. Premier or Ministerial involvement. No breakdown in key relationship.	Lost time iro temporary injury (incapacity leave). Local but lingering poor morale. Serious skills mix issues. Medium employee turnover.	
4	Immaterial	Loss of assets, adverse impact on annual revenues.	Easily remedied, some impact on external stakeholders	Temporary negative impact on reputation. Media coverage in	Lost time iro temporary injury (normal sick leave) Local but	Non-compliance with policy and procedures results in ineffective

SCORE	GRADING	FINANCIAL	SERVICE DELIVERY	REPUTATION & IMAGE	EMPLOYEE WELLNES	LEGAL/REGULARITY/ COMPLIANCE
		Financial loss of 20 – 29% of budget.	KRA's delayed.	city/provincial level for less than a week.	lingering poor morale. Skill mix issues.	procedures that impact on the KRA's.
3	Minor	Loss of assets, adverse impact on annual revenues. Financial loss of 10 – 19% of budget.	Easily remedied, some impact on internal stakeholders KRA's delayed.	One off media coverage in city/provincial level only.	Lost time injury 2 days or less. Local but lingering poor morale. Minor skill mix issues.	
2	Insignificant	Insignificant loss of assets or insignificant adverse impact on annual revenues. Financial loss of 5 – 9% of budget.	Small delay, internal inconvenience only. Can be remedied internally immediately.	Once off media coverage in community circulation only.	Minor injury. Temporary poor morale within the component.	Slight deviation from prescripts. Can be remedied internally immediately.
1	Negligible	Insignificant loss of assets or insignificant adverse impact on annual revenues. Financial loss of 0 – 4% of budget.	Internal inconvenience only. Can be remedied internally immediately.	Customer complaint received.	Minor injury Minor morale issues.	

LIKELIHOOD RATING SCALE

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

In simple terms: How likely is it that the risk or event will occur.

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

The likelihood of occurrence will be assessed as follows:

RATING	GRADING	DESCRIPTION
10	Certain	Adverse event/opportunity will definitely occur.
9	Almost Certain	There is little doubt that the event will occur. History of occurrence internally and/or at similar institutions.
8	Probable	Highly likely that adverse event/opportunity will occur.
7	Expected	The adverse event/opportunity can be expected to occur.
6	Possible	It is more likely that adverse event/opportunity will occur than not.
5	Potential	There is a 50% probability of occurrence.
4	Occasional	Unlikely, but can reasonably be expected to occur.
3	Remote	Unlikely, but there is a slight possibility that the event will occur.
1-2	Improbable	Highly unlikely that adverse event/opportunity will occur.