RISK MANAGEMENT STRATEGY

Table of contents

1. INTRODUCTION

The risk management strategy outlines a high level plan on how the Municipality will go about implementing its risk management policy. The risk management strategy is informed by the risk management policy.

The risk management strategy and risk management implementation plan are developed together to ensure connectivity and continuity. Both documents should be approved and reviewed on an annual basis.

2. DEFINITION OF RISK MANAGEMENT

Risk management is a continuous, proactive and systematic process, effected by a Council, accounting officer/ Municipal Manager, management and other personnel, applied in strategic planning and across the municipality, designed to identify potential events that may affect the department, and manage risks to be within its risk tolerance, to provide reasonable assurance regarding the achievement of the GTM objectives.

3. COMPONENTS OF RISK MANAGEMENT

The process of managing risk is a structured approach for incorporating risk management into the daily, broader management process. Risk management is more than an exercise of risk avoidance. It is as much about identifying opportunities as avoiding or mitigating losses.

Risk management is an ongoing process at every level, and consists of eight interrelated components, namely:

3.1   The Control Environment;
3.2   Objective Setting
3.3   Risk Identification
3.4   Risk Assessment
3.5   Risk Responses
3.6   Information and Communication
3.7   Control Activities
3.8   Monitoring

3.1 Control Environment

The municipal's control environment is the foundation of risk management, providing discipline and structure. The control environment influences how strategy and objectives are established, municipal 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 Municipality shall at all times, promote a positive control environment, which comprise amongst others the establishment of ethical values, competence building and development of personnel, proper delegations of authority and responsibility.

The Municipality will further establish risk management as part of the strategic and daily operations of the Municipality. Risk tolerance level shall be set for each key activity during the strategic and IDP planning process.

A code of conduct, policies and procedures shall be communicated to all staff members and action taken against those who fail to comply with the set policies and the code of conduct.

A performance management system shall be put in place and implemented. Such a performance management system shall include the assessment of management on risk management.

The Municipality shall conduct a control environment survey once in every three years. The survey shall assess, amongst others the following:

- Risk Management philosophy and culture
- Integrity and ethical values
- Organisational structure (planning, executing, control and monitoring)
- Delegation of authority and responsibility
- Committed to comply with Acts, policies and procedures.
- Staff competency
- Strategic Planning processes, etc

3.2   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 aligns the objectives with the Municipal's mission/vision and is consistent with the municipal's risk tolerance. The setting of these objectives is usually completed during the, "IDP planning and Budgetary process."

Municipal objectives can be viewed in the context of the following five categories:

Strategic – relating to high-level goals, aligned with and supporting the Municipal's mission/vision;

Operations – relating to effectiveness and efficiency of the Municipal's operations, including performance and service delivery goals.

Reporting – relating to the effectiveness of the Municipal's reporting. They include internal and external reporting and may involve financial or non-financial information;

Compliance – relating to the Municipal's compliance with applicable laws and regulations;

Safeguarding of assets – relating to prevention of loss of the municipal's assets or resources, whether through theft, waste or inefficiency. Safeguarding of assets also include the prevention or timely detection of unauthorized acquisition, use, or disposition of the municipal's assets.

Risk and exposures shall be identified in the formulation of objectives.

3.3   Risk Identification

During the phase of risk identification, management considers external and internal, as well as financial and non financial factors that influence the municipal's policy and management agenda. Identifying major trends and their variation over time is particularly relevant in providing early warnings.

Some external factors to be considered for potential risks include:
- Political: the influence of international governments and other governing bodies;
- Economic: international, national markets and globalizations;
- Social: major demographic and social trends, level of citizen engagement; and
- Technological.

Internal factors reflect management's choices and include such matters as:
- The overall management framework;
- Governance and accountability frameworks;
- Level of transparency required;
- Values and ethics;
- Infrastructure;
- Policies, procedures and processes;
- Human resource capacity; and
- Technology.

The specific internal factors for the Greater Tubatse Municipality' risk management identification shall be determined by reference to the following internal Municipal's:

- Strategic Objectives and Performance Plans;
- Organisational structure and therefore the various business units;
- Legislative and regulatory requirements;
- Previous Financial statements, annual reports;
- Auditor General reports;
- Fraud and corruption related incidents;
- Budget information;
- Organisational Policies and Procedures etc

Business Process Identification and Description

This includes:

- Establishing Management objectives and plans for each functionality or business unit;
- A description and mapping of the business processes;
- Identifying the business processes within each critical activity and
- Identifying value drivers

Other possible methods of identifying risks, sources of risk, and areas of risk impact as well key questions that can be used to identify and control risks are attached as **"appendix ii"** of this framework.

3.4   Risk Assessment

Risk assessment allows the GTM to consider how potential events might affect the achievement of objectives. Management assesses events by analysing the likelihood and its impact.

Formal Risk Assessments

The Management of the GTM shall conduct formal Risk Assessments at least annually, as required in terms of the Municipal Finance Management Act and Treasury Regulations. Risk assessment workshops will be conducted as follows:

- A separate workshop for strategic risk assessment
- Workshop for operational risk assessment

The results or information collected from the workshops will be collated and the GTM's risks database updated accordingly.

The timing of the annual formal risk assessment must fall before commencement of the annual budget process. This is intended to enable the financing of the risk management strategies and control systems that should be implemented in order to mitigate identified risks.

Continuous and Quarterly Risk Assessments

Risk assessments should be conducted for all new activities, to ensure that adequate systems are designed to address emerging risks.

Management of each business unit will be required to continuously assess the risks associated with the activities of their units. The basis for management decisions must therefore include the results of their assessments of associated risks, and the expected outcomes.

Management will therefore be required to submit quarterly reports of the risk profiles of their units. The Directors should submit the quarterly reports to the Risk Management Committee on or before due dates communicated for submission of these reports.

The risk assessment process includes 4 steps:

Step 1: Quantifying the parameters (scoring system) of impact and likelihood before the actual assessment (see the example below);

RISK RATING TABLES

TABLE A   : IMPACT

How significant the effect of risk could be on the output /objectives.

Rating	Assessment	Definition
5	**Critical**	Loss of ability to sustain ongoing operations-leads to termination of the project
4	**Major**	Significant impact on achievements of strategic objectives and targets relating to the organizational plan
3	**Moderate**	Disruption of normal operations with limited effect on achievement of strategic objectives or target relating to the organizational plan
2	**Minor**	No material impact on achievement of the organization's strategic objectives
1	**Insignificant**	Negligent impact/Minimal impact

TABLE B   : LIKELIHOOD

What are the chances that the risks will materialise?

Rating	Assessment	Definition
5	**Common**	The risk is either already occurring, or is almost certain to occur more than once within the next 12 months. (Probability = 80≥100%
4	**Likely**	The risk is almost certain to occur once within the next 12months. (Probability = 50≥80%
3	**Moderate**	The risk could occur at least once in the next 2 years. (Probability = 10≥ 50%)
2	**Unlikely**	The risk could occur at least once in the next 10 years. (Probability = 1≥10%)
1	**Rare**	The risk will probably not occur. (Probability = 0-1%)

Step 2: Applying the parameters to the risk matrix to indicate what areas of the risk matrix would be regarded as high, medium or low risk (see the example below);

TABLE C
Risk index = impact x likelihood

I	5	10	15	20	25
M	4	8	12	16	20
P	3	6	9	12	15
A	2	4	6	8	10
C	1	2	3	4	5
T		**LIKELIHOOD**			

Risk index	Risk Magnitude
15 – 25	High risk
10 – 14	Medium risk
1 -9	Low risk

Step 3: Determining the risk acceptance criteria by identifying what risks will not be tolerated (see **the example below);**

The following is a rating table that can be utilised to categorise the various levels of inherent risk

Risk rating	Inherent Risk Magnitude	Response
15 - 25	High	Unacceptable level of risk – High level of control intervention required to achieve an acceptable level of residual risk
10 – 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
1 -9	Low	Mostly acceptable – Low level of control intervention required, if any

What is acceptable risk?

Determining that a risk is acceptable does not imply that the risk is insignificant. A risk may be considered to be acceptable because:

- The threat posed is assessed to be so low (for an example because the likelihood of occurrence is rare) that specific treatment is not necessary;

- The risk is such that the Municipality has no available treatment, for an example, the risk of a change to a particular project might occur following a change of Government;

- The cost of treating the risk is so high compared to the benefit from successful treatment; or

- The opportunities presented outweigh the threats to such an extent that the risk is justified.

Step 4: Determine control effectiveness and residual risk ratings

TABLE D: CONTROL EFFECTIVENESS

Rating	Effectiveness	Definition
0.20	Always Effective	Risk Exposure is effectively controlled and managed
0.40	Mostly Effective	Majority of risk exposure is effectively controlled and managed.
0.50	Partially Effective	There is room for some improvement
0.70	Almost Ineffective	Some of risk exposure appears to be controlled, but there are major deficiencies.
0.90	Poor/Ineffective	Control measures are ineffective.
1.0	No Control	There is no control measure in place

Residual risk exposure (Inherent Risk x Control Effectiveness)

a) Control is very good/ always effective = 0.20

If inherent risk rating is **25** i.e. (impact=5 x likelihood=5), then the residual risk will be

5 = (25 X 0.2)

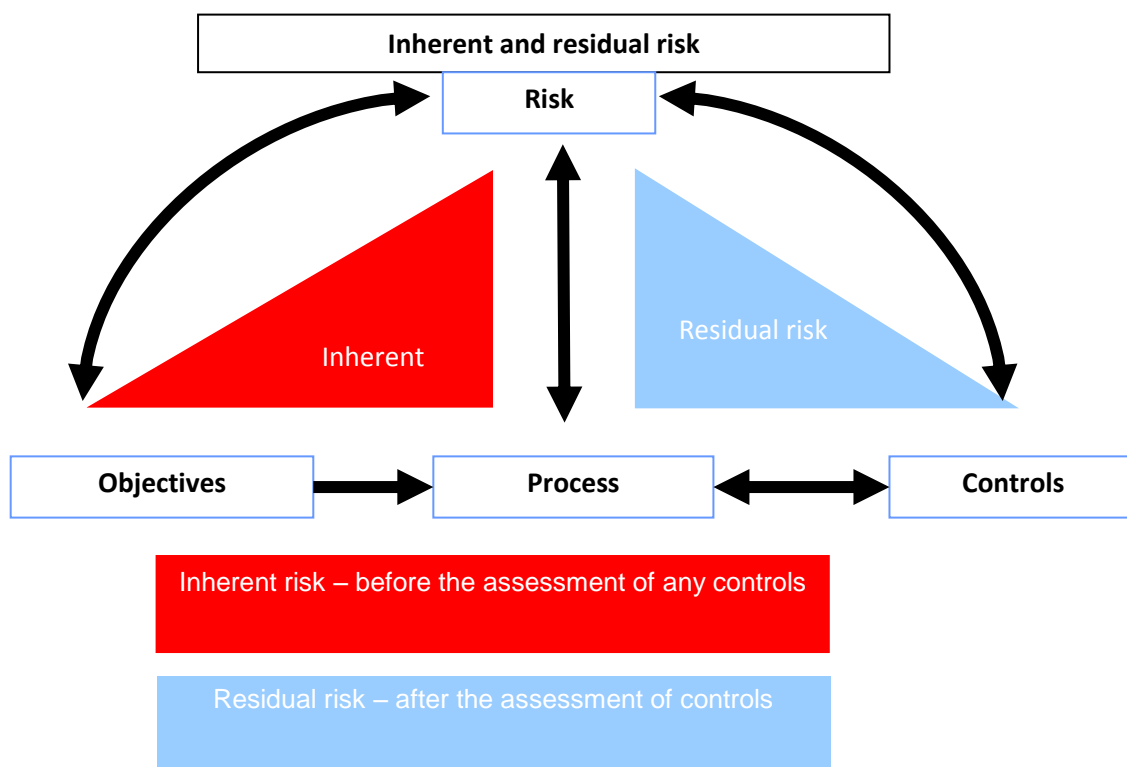***b) Control is poor/ ineffective = 0.90***

If inherent risk rating is **25 i.e.** (impact=5x likelihood=5), then the residual risk will be **22.5** (25 X 0.9)

The following is an example of the rating table that will be used to categorise the various levels of residual risk.

Risk rating	Residual risk magnitude	Response
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.
10 – 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.
1 - 9	Low	Mostly acceptable level of residual risk – Requires minimal control improvements.

The following diagram differentiates between inherent and residual risk:

Inherent and residual risk

```
                        Risk
```

Inherent

Residual risk

| Objectives | Process | Controls |

Inherent risk – before the assessment of any controls

Residual risk – after the assessment of controls

3.5   Risk Responses

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 Municipal's risk tolerance levels. However, not all risks will require treatment as some may be accepted by the Municipality and only require occasional monitoring throughout the period.

The risks that fall outside of the Municipal's risk tolerance levels are those which pose a significant potential impact on the ability of the Municipality to its 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.

a) The risk response plan usually provides detail on:
   i.   actions to be taken and the risks they address;
   ii.   who has responsibility for implementing the plan;
   iii. what resources are to be utilized;
   iv.   the budget allocation;
   v.   the timetable for implementation;
   vi.   details of the mechanism and frequency of review of the status of the response plan.

11

b) Responding to risks involves the following key steps;

    i.   Identify risk response options
    ii.   Select risk response options
    iii.   Assign risk ownership
    iv.   Prepare risk response plans

c) The following risk response options which are self-explanatory should be considered and can be understood to mean the following:

    i.   **Risk avoidance response**- take action to remove the activities that give rise to the risks. Avoiding it altogether by not investing any of the municipal's resources.

    ii.   **Risk reduction response** – measures to reduce the threat posed by the risk, either by reducing the likelihood of the risk and/or its impact, or both.

    iii.   **Risk sharing response**-transferring the threat by shifting the risk to another party via, for example, contracting out or insurance.

    iv.   **Risk acceptance response** –accepting the risk without taking any action to avoid it, but monitoring the risk and ensuring that the Municipality has the financial and other capacities to cover associated losses and disruptions.

Management shall identify risk response options, which should include a fraud prevention plan, and consider their effect on event likelihood and impact, in relation to risk tolerances, costs versus benefits, and thereafter designs and implements response options..

d) The following key mechanisms will form part of the GTM strategy to manage the risks of potential corruption and or fraud:

    i.   Fraud Risk Assessment
    ii.   Anti Fraud and Corruption Policy & Fraud Prevention Plan
    iii.   Fraud Awareness Programme
    iv.   Whistle-Blowing Mechanism
    v.   Fraud Detection Mechanisms
    vi.   Strategic Partner(s) for Forensic Investigations

In line with the responsibility for the management of risks, as outlined in risk management policy, management shall be responsible for the detection and prevention of the risks of fraud and corruption.

3.6   Information and Communication

The Risk Management Committee shall be responsible for evaluating and adopting the methodology of assessing risk appetite and/or risk tolerance and make recommendations to the Municipal for the approval thereof.

Risk tolerance levels may be set at Risk Category levels and/or business unit levels.

Risk Category	Risk Tolerance Levels	Risk Appetite
Internal Risks Human resources Knowledge and Information Management Litigation Loss/theft of assets Procurement risk Service delivery Information technology Third party performance Health & Safety Disaster recovery/business continuity Compliance/regulatory Fraud & corruption Financial Cultural	Risk rating from 1-9: Acceptable Risk rating from 10-25: Unacceptable	Risk 1- 9 = Low Risks Risk 10-14 = Medium Risks Risk 15-25 = High Risks
External Risks Reputation Economic environment Political environment Social environment Natural environment Technological environment Legislative environment	Risk rating from 1-9: Acceptable Risk rating from 10-25:Unacceptable	Risk 1-9 = Low Risks Risk 10-14 = Medium Risk Risk 15-25 = High Risks

Risks that are considered significant, material and / or fundamental (high risks) will be reported to the Audit Committee at each Audit Committee meeting. The Audit Committee shall give assurance as to the effectiveness of the risk management strategies.

The management of these risks and the effectiveness of the strategies adopted to mitigate the risks will be escalated to the Accounting Officer. The Municipality will periodically report to the relevant

structures including Risk Management Committee, Exco and Council on all risks that are of a significant nature.

The risk profile of the Municipality must be communicated to all managers within the Greater Tubatse Municipality. Managers should communicate to their staff the risk levels that are acceptable to each task or activity and the strategies that are designed to mitigate the risks. The communication of the risk profile should be guided by the need for the employees of the Municipality to understand their role in and contributions to the Greater Tubatse Municipality's risk appetite.

3.7   *Control Activities*

Control activities are part of the process by which the Municipality strives to achieve its business objectives. Control activities are the policies and procedures that help ensure risk management strategies are properly executed. They occur throughout the municipality, at all levels and in all functions.

They usually involve two elements: a policy establishing what should be done and procedures to effect the policy.

3.7.1   Internal Control

Internal control is an integral part of risk management. This strategy encompasses internal control, forming a more robust conceptualization and tool for management. The Greater Tubatse Municipality shall adopt an integrated Internal Control Framework, which shall be aligned to best practice. Internal Control shall be defined as those elements of the municipality, including its resources, people, systems, processes, culture, structure and tasks, which taken together, support the achievement of the organization's objectives. Alternatively, internal control shall be defined as a process effected by management, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Safeguarding of assets
- Compliance with applicable laws and regulations

Control procedures relate to the actual policies and procedures in addition to the control environment that management has established to achieve its objectives. Policies and procedures help create boundaries and parameters to authority and responsibility, and also provide some scope of organisational precedent for action.

3.7.2   Control Procedures

Specific control procedures include:

- Reporting, reviewing and approving reconciliations;
- Checking the arithmetical accuracy of records;
- Controlling applications and environment of computer information systems;
- Maintaining and reviewing control accounts and trial balances;

- Approving and controlling documents;
- Comparing internal data with external sources of information;
- Comparing the result of cash, security and inventory counts with accounting records
- Comparing and analysing the financial result with budgeted amounts
- Limiting direct physical access to records

Control can help minimize the occurrence of errors and breakdowns, but cannot provide absolute assurance that they will not occur, and the system of internal control as listed below should be embedded in the operations of the department and form part of its culture.

3.7.3   Broad Internal Control Focus Areas

Internal controls established in a municipality should focus on the following areas:

3.7.3.1 Adequate segregation of duties
Key duties and responsibilities in authorizing, processing, recording, and reviewing transactions and events should be separated among individuals;

3.7.3.2 Custody and accountability for resources
Access to resources and records are to be limited to authorized individuals who are accountable for their custody or use;

3.7.3.3 Prompt and proper recording and classification of transactions
Transactions should be recorded and properly classified to ensure that information maintains its relevance and value to management in controlling operations and decision-making and to ensure that timely and reliable information is available to management;

3.7.3.4 Authorization and execution of transactions
Requires that employees execute their assigned duties in accordance with directives and within the limitations established by management or legislation;

3.7.3.5 Documentation
Internal control structures, i.e. policies and procedures, and all transactions and significant events are to be clearly documented;

3.7.3.6 Management supervision and review
Competent supervision is to be provided, including assignment, review and approval of an employee's work.
Employees should be provided with the necessary guidance and training to help ensure that errors, wasteful, and wrongful acts are minimized and that specific management directives are understood and achieved.

The Greater Tubatse Municipality should implemented the following computer controls:

3.7.4   Access Controls

These are controls that should designed to prevent:

- Unauthorized changes to programs which process data;
- Access to files which store accounting and financial information and application programs;
- Access to computer operating systems and system software programs;
- User-id's and passwords should be used to limit access to programs, data files and software applications;
- Firewalls should be installed to prevent data corruption from unauthorized external access.

3.7.4.1 System Software Programs

Controls should be designed for programs, which do not process data to ensure that they are installed or developed and maintained in an authorized and effective manner, and that access to system software is limited.

This could be achieved through security over system software, database systems, networks and processing by users on personal computers. There should be support structures, error correction methods and adequate documentation for the systems.

Controls should be designed to ensure the continuity of processing, by preventing system interruption or limiting this to a minimum.

Controls that should be in place include physical protection against the elements such as fire, water and power. There should be emergency plan and disaster recovery procedures, provision of alternative processing facilities, backups of data files, maintenance of hardware, adequate insurance, cable protection, uninterruptible power supply, prevention of viruses and personnel controls affecting security and continuity.

3.7.4.2 Information systems controls

With widespread reliance on information systems, controls are needed over significant systems. Two broad groupings of information systems control activities can be used. The first is general controls, which apply to many if not all application systems and help ensure their continued, proper operation. The second is application controls, which include computerized steps within application software to control the technology application. Combined with other manual process controls where necessary, these controls ensure completeness, accuracy and validity of information.

3.7.5   General Controls

General controls include;

- controls over information technology management, which will address the information technology oversight process, monitoring and reporting information technology activities, and municipal improvement initiatives. Other controls

- information technology infrastructure, security management and software acquisition, development and maintenance. These controls apply to all systems from mainframe to client/server to desktop computing environments.

3.7.6 Application Controls

Application controls are designed to ensure completeness, accuracy, authorization and validity of data capture and transaction processing. Individual applications may rely on effective operation of controls over information systems to ensure that interface data are generated when needed, supporting applications are available and interface errors are detected and corrected timeously.

The controls are designed to manage the operation of the system and to ensure that programmed procedures are applied correctly and consistently during the processing of data.
Computer controls such as scheduling of processing time, execution of programs by competent personnel, monitoring and review of the function of hardware, division and rotation of duties and maintenance of system and manual logs with regular follow-up management should be available.

3.8 Monitoring

The Risk database in which all the information from the risk management processes will be stored; will be used as one of the tools to monitor:

The authority to update the Municipal Risks Database shall be restricted to designated officials.

In future a Risk Management software solution will be acquired for capturing and reporting the overall risk management process. This will be done in conjunction with IT unit in terms of providing the necessary technological support.

Control Self Assessment questionnaires, Internal Audit and other independent assurance providers will be used as a tools to assess the effectiveness of the internal control and other risk management strategies that have been designed and implemented by management.

The Risk Management Committee of the Municipality should benchmark the GTM's risk management practices and performance against best practice. As a reporting procedure, the following methods will be applied;

- The quarterly reports on risk management should include a top ten (10) high risks and the management thereof.
- The Risk Management Committee should report on the risks per each category in the risk management strategy.

APPENDIX I

THE DEFINITIONS OF RISK AND RISK MANAGEMENT

RISK

Risk is "any uncertain event or set of circumstances that, should it occur or fail to occur, would have an effect on the ability to meet the organisation's objectives".

The main components of risk therefore are:

- The probability of occurrence or non-occurrence
- The root cause of the uncertainty
- The qualitative or quantitative impact.
- Control effectiveness

The risks of the GTM shall be classified into Strategic Risks, Business Risks, Operational Risks and Process Risks.

Strategic Risks

Strategic Risks are external and internal forces that may have a significant impact on achieving key strategic objectives. The causes of these risks include such things as national and global economics and most significantly. Often they cannot be predicted or monitored through a systematic operational procedure. The lack of advance warning and frequent immediate response required to manage strategic risks means they are often best identified and monitored by senior management as part of strategic planning and review mechanism.

Business Risks

Risks attached to the decision-making, operations and actions at the strategic management level.

Operational Risks

Operational risks are inherent in the ongoing activities that are performed in an organisation. These are the risks associated with such things as the day to day operational performance of staff, the risk inherent in the organisational structure, and the manner in which core operations are performed.

RISK MANAGEMENT

Risk Management is a continuous process that can be defined as:

- The identification and assessment of actual and potential risks that the organization may be exposed to,
- Ensuring that appropriate structures, policies and procedures are in place to manage these risks, and

- The design and introduction of controls to pro-actively manage or mitigate the risk probability and impact.

This assessment requires management decisions to accept, avoid, transfer or control the risks, or a combination of these options. Risk Management also includes the identification of areas of opportunity, and therefore the risks that should be taken in pursuance of these opportunities, with appropriate strategies to mitigate against avoidable losses.

APPENDIX II

Possible Methods of Identifying Risks

- Interview/focus group discussion;
- Audits or physical inspections;
- Brainstorming;
- Survey, questionnaire,
- Examination of local and/or overseas experience;
- Networking with peers, industry groups and professional associations;
- Judgmental – speculative, conjectural, intuitive;
- History, failure analysis;
- Examination of personal experience or past department or public entity experience;
- Incident, accident and injury investigation;
- Databank of risk events which have occurred;
- Scenario analysis;
- Decision trees;
- Strengths, weaknesses, opportunities, threats (swot) analysis;
- Flow charting, system design review, systems;
- Analysis, systems engineering techniques e.g. Hazard and operability (hazop) studies;

Possible Sources of Risk

- New activities and services;
- Disposal or cessation of current activities;
- Outsourcing to external service providers;
- Commercial/legal changes;
- Changes in the economic conditions;
- Socio-political changes, like elections;
- National and international events;
- Personnel/human behaviour;
- Behaviour of contractors/private suppliers;
- Financial/market conditions;
- Management activities and controls;
- Misinformation;
- Technology/technical changes, i.e. New hardware and software implementations;
- Operational (the activity itself) changes;
- Department interruption;
- Occupational health and safety;
- Property/assets;
- Security (including theft/fraud);
- Natural events;
- Public/professional/product liability

Key questions that can be used to identify and control risks

- What, when, where, why and how risks are likely to occur, and who might be involved?
- What is the source of each risk?
- What are the consequences of each risk?
- What controls presently exist to mitigate each risk?
- To what extent are controls effective?
- What alternative, appropriate controls are available?
- What are the department obligations – external and internal?
- What is the need for research into specific risks?
- What is the scope of this research, and what resources are required?
- What is the reliability of the information?
- Is there scope for bench-marking with peer organizations?

APPENDIX III

RISK CLASSIFICATION

A Risk Classification is a master list that enables the categorization of all risks identified.

The main categories in the Municipal's Risk classification, in the attached table will include:

- Human Resources
- Knowledge and information management
- Litigation
- Loss/theft of assets
- Procurement risk
- Service delivery
- Information Technology
- Third party performance
- Health and safety
- Disaster recovery/business continuity
- Compliance/Regulatory
- Fraud and Corruption
- Financial
- Cultural
- Reputation
- Economic Environment
- Political Environment
- Social Environment
- Natural Environmental
- Technological Environment

Management of the Department may recommend changes to the Risk Classification for approval by the Risk Management Committee.

Any changes to the Risk Classification will not constitute a change in the Risk Management Strategy.

RISK CATEGORISATION TABLE

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 and honesty; • Recruitment; • Skills and competence; • Employee wellness; • Employee relations; • Retention; and • Occupational health and 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 party • 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.

Risk Type	Risk Category	Description
Internal	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
	Service delivery	Every institution exists to provide value for its stakeholders. The risk will arise if the appropriate quality of service is not delivered to the citizens.
	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.
		Inadequate / poor quality of performance.

Risk Type	Risk Category	Description
Internal	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.

Risk Type	Risk Category	Description
External	Cultural	Risks relating to an institution's overall culture and control environment. The various factors related to organizational 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.
	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.

Risk Type	Risk Category	Description
	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.

APPENDIX IV

GLOSSARY OF RISK MANAGEMENT TERMS

Risk

Risk is "any uncertain future event or set of circumstances that, should it occur or fail to occur, would have an effect (either positive or negative) on the ability to meet the objectives". A risk is often specified in terms of an event or circumstances and the consequences that may flow from it. It is measured in terms of a combination of the consequences of an event and their likelihood. Note that risk is characterized by uncertainty.

Risk Assessment

Refers to overall process of identifying, analysing and evaluating risks. It may also be referred to as a "risk analysis" or risk "evaluation" and may involve a qualitative and/or quantitative assessment.

Inherent Risk

Inherent risk is the risk attached to a business process *before taking into account* any existing internal controls. It is a risk that exists because the process exists.

Impact

Impact refers to the significance of the effect that the identified risk may have on the activities, should management not adequately and effectively control them.

Likelihood/Probability of Occurrence

Likelihood refers to the probability of the occurrence of a risk within an activity of the process.

Risk Register

A risk register is a document record of all risks identified as part of risk assessment (also known as risk profile). It can be in a form of an electronic database

Control Self Assessment

Control Self Assessments is a tool or technique in the form of questionnaires that is used as the department's self-evaluation of the success or otherwise of the strategies that they will have implemented to manage the identified risks; and therefore the ability to achieve the department's objectives.

Management shall have the authority to use their own discretion on the frequency of the control self-assessments. However, formal control-self-assessments shall be conducted at least every six (6) months during a given financial period.