IT RISK MANAGEMENT POLICY

1. Purpose of this document

- The policy forms part of the municipality's internal control and governance arrangements.
- The policy explains the underlying approach to IT Risk management, documents the roles and responsibilities of the IT Steering Committee and other key parties. It also outlines key aspects of the risk management process, and identifies the main reporting procedures.
- In addition, it describes the process the Steering Committee will use to evaluate the effectiveness of the internal control procedures.

2. Role of the Steering Committee

The IT Steering Committee has a fundamental role to play in the management of risk. The IT Steering Committee has responsibility for overseeing risk management within the municipality as a whole.

Its role is to:

- communicating the municipality's approach to risk
- determining what types of risk are acceptable and which are not
- Determine the appropriate risk appetite or level of exposure for the risk
- Approve major decisions affecting the risk profile or exposure.

- Identify risks and monitor the management of fundamental risks to reduce the likelihood of unwelcome surprises.
- Satisfy itself that the less fundamental risks are being actively managed, with the appropriate controls in place and working effectively.
- Annually review the municipality's approach to risk management and approve changes or improvements to key elements of its processes and procedures.

3. Roles of Information technology:

- Implement policies on IT risk management and internal control.
- Identify and evaluate the fundamental risks faced by the municipality for consideration by the Steering Committee.
- Information technology must provide adequate information in a timely manner to the IT Steering Committee and its sub-committees on the status of risks and controls.
- Undertake an annual review of effectiveness of the system of internal control and provide a report to the IT Steering Committee.

4. Risk management as part of the system of internal control

The system of internal control incorporates risk management. This system encompasses a number of elements that together facilitate an effective and efficient operation, enabling the municipality to respond to a variety of operational, financial, and commercial risks. These elements include:

a. Policies and procedures.

Attached to fundamental risks are a series of policies that underpin the internal control process. The policies are set by the IT Steering Committee and implemented and communicated to staff.

b. Reporting

Comprehensive reporting is designed to monitor key risks and their controls. Decisions to rectify problems are made at regular meetings of the Steering Committee.

c. Risk Management Process.

The municipality operates a risk management process/framework as follows:

- A review/appraisal of the previous year's risk management report
- A 'risk identification' exercise for the year ahead
- Evaluation of identified risks using risk assessments
- Manage risks through application of risk management techniques
- Record and monitor risks using risk registers
- Assigning responsibility for risks to appropriate personnel.

Risk identification is not an annual process. IT Steering Committee members are encouraged to report and update risk registers and carry out assessments throughout the year.

d. Annual review of effectiveness

The Steering Committee is responsible for reviewing the effectiveness of internal control of the municipality, based on information provided by the IT. Its approach is outlined below.

For each fundamental risk identified, the board will:

- review the previous year and examine the municipality's track record on risk management and internal control
- Consider the internal and external risk profile of the coming year and consider if current internal control arrangements are likely to be effective.

In making its decision the IT Steering Committee will consider the following aspects.

a. Control environment:

- the municipality's objectives and its financial and non-financial targets
- organisational structure and calibre of the staff
- culture, approach, and resources with respect to the management of risk
- delegation of authority
- Public reporting.

b. On-going identification and evaluation of fundamental risks:

- timely identification and assessment of fundamental risks
- Prioritisation of risks and the allocation of resources to address areas of high exposure.

c. Information and communication:

- quality and timeliness of information on fundamental risks
- Time it takes for control breakdowns to be recognised or new risks to be identified.

d. Monitoring and corrective action:

- ability of the municipality to learn from its problems
- Commitment and speed with which corrective actions are implemented.
- The delegated member of staff responsible for risk management will prepare a report of its review of the effectiveness of the internal control system annually for consideration by the IT Steering Committee.

5. RISK IDENTIFICATION

This step to identify the risks to the IT system. Risks occur in IT systems when Vulnerabilities (i.e., flaws or weaknesses) in the IT system or its environment can be exploited by threats (i.e. natural, human, or environmental factors).

The process of risk identification consists of three components:
1. Identification of vulnerabilities in the IT system and its environment;
2. Identification of credible threats that could affect the IT system; and
3. Pairing of vulnerabilities with credible threats to identify risks to which the IT system is exposed.

After the process of risk identification is complete, likelihood and impact of risks will be considered.

Determination of the risks rating guide

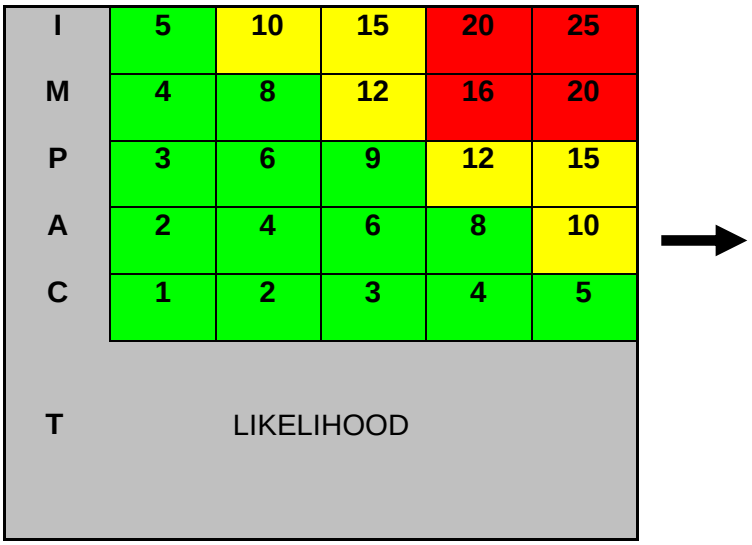
RATING GUIDE – LIKELIHOOD

Rating	Assessment	Definition
1	Rare	The risk is conceivable but is only likely to occur in extreme circumstances
2	Unlikely	The risk occurs infrequently and is unlikely to occur within the next 3 years
3	Moderate	There is an above average change that the risk will occur at least once in the next 3 years
4	Likely	The risk could easily occur and is likely to occur at least once within the next 12 months
5	Common	The risk is already occurring, or is likely to occur more than once within the next 12 months

RATING GUIDE – IMPACT

Rating	Assessment	Definition
1	Insignificant	Negative outcomes or missed opportunities that are likely to have a SLIGHT IMPACT on the ability to meet objectives
2	Minor	Negative outcomes or missed opportunities that are likely to have a RELATIVELY LOW IMPACT on the ability to meet objectives
3	Moderate	Negative outcomes or missed opportunities that are likely to have a RELATIVELY MODERATE IMPACT on the ability to meet objectives
4	Major	Negative outcomes or missed opportunities that are likely to have a SIGNIFICANT IMPACT on the ability to meet objectives
5	Critical	Negative outcomes or missed opportunities that are of CRITICAL IMPORTANCE to the achievement of the objectives

Risk Rating = impact x likelihood



Risk Rating = impact x likelihood

RISK RATING	PRIORITY
16 - 25	HIGH
10 - 15	MEDIUM
1 - 9	LOW

IT Sector are systematically addressing the risks of concern for each critical function by engaging in risk management analyses wherein assess the merits and drawbacks of taking one of four approaches to risk mitigation:

- Avoid the risk;
- Accept the risk and its potential consequences;
- Transfer the risk to another entity, capability, or function; or
- Mitigate the risk by preventative or proscriptive action.

Where mitigation is the preferred risk response, IT Sector will identify appropriate Risk Mitigation Activities (RMA) to reduce national-level risks across each critical function. The identified risk responses and the prioritization of the mitigations identified for IT risks will inform resource allocation to most effectively respond to the threats, vulnerabilities, and/or consequences facing the critical IT functions.

Four major concerns could lead to confidential information disclosure:

- Negligent use or mismanagement of files, such as monitoring logs, disconnected and discarded hard drives
- Poor or negligent software development practices
- Phishing attacks
- Non-secure wireless networks