UMZIMVUBU

LOCAL MUNICIPALITY

ICT RISK MANAGEMENT POLICY

Table of Contents

Terms and Definitions

Asset	Anything that has value to the organization
Availability	The property of being accessible and usable upon demand by an authorized entity
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, entities, or processes
Control	Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature
Guideline	A description that clarifies what should be done and how, to achieve the objectives set out in policies
Information security	Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, nonrepudiation and reliability can also be involved
Information security event	An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant
Information security incident	A single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security
Information security management system	That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security **NOTE**: The management system includes organizational structures, policies, planning activities, responsibilities, practices, procedures, processes and resources
Integrity	The property of safeguarding the accuracy and completeness of assets
Policy	Overall intention and direction as formally expressed by management
Risk	Combination of the probability of an event and it's consequence
Residual risk	The risk remaining after risk treatment
Risk acceptance	Decision to accept a risk
Risk analysis	Systematic use of information to identify sources and to estimate the risk
Risk assessment	Overall process of risk analysis and risk evaluation
Risk evaluation	Process of comparing the estimated risk against given risk criteria to determine the significance of the risk
Risk management	Coordinated activities to direct and control an organisation with regard to risk
Risk treatment	Process of selection and implementation to measures to modify risk

Third party	That person or body that is recognized as being independent of the parties involved, as concerns the issue in question
Threat	A potential cause of an unwanted incident, which may result in harm to a system or organization
Vulnerability	A weakness of an asset or group of assets that can be exploited by one or more threats

Preamble

The Municipality is committed to the governance of information and communication technologies within the Municipality so as to manage strategy, manage enterprise architecture, manage portfolios, manage suppliers, manage risk and manage security. The Municipality intends to ensure that stakeholder needs are met and to align business needs and information technology needs, specifically:

- The municipality will develop and maintain high-quality information to support business decisions;
- The municipality aims to generate business value from IT-enabled investments, achieving strategic goals and realising business benefits through the effective and innovative use of IT;
- The Municipality seeks to achieve operational excellence through the reliable and efficient application of information and communication technology;
- The Municipality will maintain IT-related risk at an acceptable level;
- The Municipality will optimise the cost of IT services and technology;
- The Municipality will comply with relevant laws, regulations, contractual agreements and policies.

The Municipality seeks to achieve these measures through the application of five principles, specifically:

- It will seek to meet stakeholder needs by ensuring that relevant stakeholders are identified and classified according to their needs;
- It will govern the Municipality end-to-end by integrating the governance of ICT into corporate governance, covering all the functions and processes required to govern and manage information and related technologies wherever such information may be processed;
- It will apply a single, integrated ICT governance and management framework by defining a set of governance and management enablers. These will provide a structure for all relevant guidance materials, as well as providing a comprehensive reference base of good practices;
- It will adopt and enable an holistic approach to ICT governance that includes:
    - principles, policies and frameworks
    - processes
    - organisational structures
    - culture, ethics and behaviour
    - people, skills and competencies
    - services, infrastructure and applications
    - information

It will separate governance and management, recognising that governance and management comprise different types of activities with different responsibilities; governance being the duty to evaluate, direct and monitor enterprise activities, while management is the duty to plan, build, run and monitor those activities.

The Municipal Corporate Governance of ICT Policy is based on principles as explained in international good practices and standards for ICT governance, namely, King III Code, ISO/IEC 38500 and COBIT.

The following are the principles which have been adopted in PSCGICTPF have been adapted specifically for municipalities. Now referred to as the MCGICTPF.

- Principle 1 – Political Mandate
- Principle 2 – Strategic Mandate
- Principle 3 – Corporate Governance of ICT
- Principle 4 – ICT Strategic Alignment
- Principle 5 – Significant ICT Expenditure
- Principle 6 – Risk Management and Assurance
- Principle 7 – Organisational Behaviour

As per Principle 6 above, Management must ensure that ICT risks are managed and that the ICT function is audited. Management must ensure that ICT risks are managed within the municipal risk management practice. It must also ensure that the ICT function is audited as part of the municipal audit plan.

As per the Municipal Corporate Governance of ICT Policy the Municipal Risk and Audit Committee must assist the Municipal Manager in carrying out his/her Corporate Governance of ICT accountabilities and responsibilities.

The Municipal Risk and Audit Committee is made up of nominated members of the Audit and Risk committee/s of the municipality as well as the ICT Manager. This committee has the specific responsibility to perform an oversight role for the Identification and Management of ICT audit and governance compliance, and ICT Risks.

As per Phase 1 of the MCGICTPF (The Enablement Phase), which is to be completed by June 2017, the municipality must have an approved and implemented Municipal Risk Management Policy that must include the management of ICT related risks.

The purpose of this document is to elaborate on how ICT related risks are managed. ICT related business risks are managed within the risk management culture and appetite of the Municipality. Risks will be managed according to best practice. This will involve the identification of likely risks, planning to avoid them and planning to mitigate any damage should they arise. ICT risks will be managed within the risk tolerance of the municipality.

Unforeseen risks will be responded to in a timely fashion, with all mitigation documented and assessed.

This ICT Risk Management Policy will focus on ICT Operational Risk which can be defined as risk focused on ICT Operations namely, Personnel, Technical, Cost, Schedule, Resource, Operational Support, Quality, Provider Failure, Environmental and Infrastructure Failure.

What is Risk?

Risk is the vulnerability to threats that jeopardize the confidentiality, integrity and availability of important data of any organisation.

Risk Assessment

Operational ICT Risk assessment is defined as identifying, quantifying and prioritizing risk against criteria for risk acceptance and objectives relevant to the organization.

The results of the assessment are used to guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against assessed risks.

Risk Rating = Threat Impact X Probability/Likelihood

The assessment should be performed on a quarterly basis.

Risk Assessment Approach

Each risk should be assessed systematically by estimating the magnitude of the risk (Risk Analysis) and comparing the estimated risk against the risk criteria to determine the significance of the risk (risk evaluation).

The systematic approach is as follows:
Consequence – the harm that is likely to result from a significant breach of information security, taking account of the potential consequences of loss or failure of information confidentially, integrity and availability.
Probability – the realistic likelihood of such a breach occurring in the light of prevailing threats, vulnerabilities and controls.

The Risk Analysis and Risk Evaluation (M_o_R – Management of Risk) criteria are as follows:

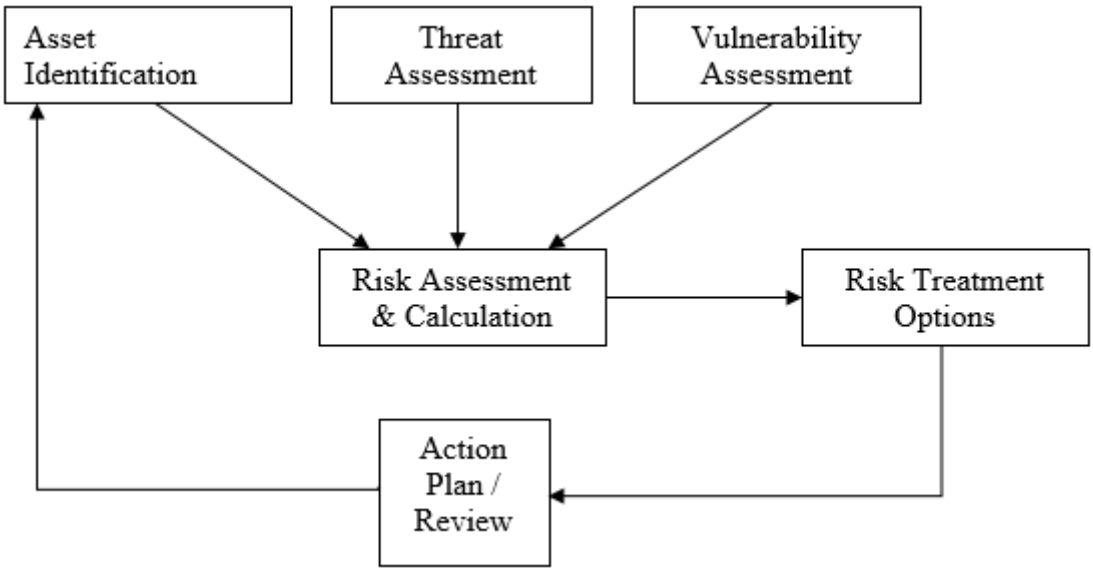
- Identify risk
- Assign risk ownership
- Assess the business harm that might result from event
- Assess the realistic likelihood of such an event
- Estimate the levels of risks
- Determine whether the risk is acceptable depending on the level (e.g. low) or requires treatment depending on the cost effectiveness of treatment versus risk level.

For each identified risk after assessment, a risk treatment decision needs to be made. Possible options for risk treatment include:

- Applying appropriate controls to reduce the risk
- Knowingly and objectively accepting risks, providing they clearly satisfy the organizations policy and criteria for risk acceptance.
- Avoiding risks by not allowing actions that would cause the risks to occur
- Transferring the associated risks to other parties, e.g. insurers or suppliers

Risk Assessment Process

The following diagram is an illustration of the risk assessment process (Adopted from an ISACA model):



Identification of Risk (This is a theoretical description of the above table), the steps involved in the identification of risks include:

- Identify assets within the scope of the Information Security Management System and the owners of these assets.
    - The first stage of the information security risk assessment process is the identification and valuation of assets, i.e. critical and/or sensitive information and data
    - An asset is something that has value or utility to the organization, its business operations and their continuity.
    - For each of the assets, values should be identified that express the business impacts if confidentiality, integrity or availability, or any other important property of the asset is damaged
    - The result of this step should be an inventory containing all assets.
- Identify the threats to those assets
    - A threat is defined as a potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm.
    - It is important to identify the weakness of any asset that supports the organization's critical data.
    - Identify the source of the threat that could lead to a breach of certain vulnerability, common threat sources are natural, human or environment.
    - The result of this step is an alignment of threats to each asset and a threat source.
- Identify the vulnerabilities that might be exploited by the threats
    - Vulnerability is defined as a flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.
    - A vulnerability in itself does not cause harm, it is merely a condition or set of conditions that may allow a threat to affect an asset
    - The goal of this step is to develop a list of system vulnerabilities (Flaws or Weaknesses) that could be exploited by the potential threat sources.
- Identify the impact that losses of confidentiality, integrity and availability may have on the assets
    - For impact to be calculate properly one need to know the system's value or importance to the organization by performing a BIA (Business Impact Analysis).
    - Before performing the impact analysis, it is necessary to obtain the following necessary information:
        - System Mission (e.g. the process performed by the IT System)
        - System & data criticality (e.g. the system's value or importance to an organisation)
        - System & data sensitivity

- The adverse impact of a security event can be described in terms of loss or degradation of any, or a combination of any, of the following three security goals:
  - Integrity
    - System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorised changes are made to the data or IT System by either intentional or accidental acts.
  - Availability and;
    - If a mission-critical IT system is unavailable to its end users, the organization's mission may be affected
    - Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impending the users' performance of their functions in supporting the organisations' mission.
  - Confidentiality
    - System and data confidentiality refers to the protection of information from unauthorised disclosure.

Magnitude of Exposure - Using all the outlined methods in the framework the magnitude of exposure of any Risk must be calculated by taking into consideration, Risk Likelihood, Risk Impact and Risk Exposure. All this information should then is populated into a Risk Register.

Risk Identification Methodology

Risk Impact Table

Rating	Assessment	Definition
1	Insignificant	Negative outcomes or missed opportunities that are likely to have a negligible 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 relatively substantial 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 Likelihood Table

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 chance 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

Inherent Risk Exposure Table

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
8-14	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
1-7	Low	Mostly acceptable – Low level of control intervention required, if any

Risk Matrix Table (Risk Tolerance Level)

IMPACT						
	Critical (5)	Manage & Monitor risks	Manage & monitor risk and have Mitigation and control strategies in place	Extensive management & monitoring essential; Mitigation and control strategies essential	Extensive management & monitoring crucial; Mitigation and control strategies crucial	Extensive management & monitoring crucial; Mitigation and control strategies crucial
	Major (4)	Accept but monitor risks	Manage & Monitor risks	Considerable management required	Extensive management & monitoring essential	Extensive management & monitoring crucial; Mitigation and control strategies crucial
	Moderate (3)	Accept but monitor risks	Risks may be worth accepting with monitoring	Management effort worthwhile	Management effort required	Extensive management & monitoring essential; Mitigation and control strategies essential
	Minor (2)	Accept Risks	Accept Risks	Accept but monitor risks	Manage & Monitor risks	Manage & Monitor risk essential
	Insignificant (1)	Accept Risks	Accept Risks	Accept Risks	Accept but monitor risks	Accept but monitor risks
		Rare (1)	Unlikely (2)	Moderate (3)	Likely (4)	Common (5)
	LIKELIHOOD					

Risk Tolerance

As per the Risk Matrix Table above the lowest possible rating to be allocated to a risk is 1 (Impact is Insignificant (1) X Likelihood is Rare (1)). The highest possible rating to be allocated to a risk is 25 (Impact is Critical (5) X Likelihood is Common (5)).

The Risk Matrix Table above should be updated on a regular basis to ensure that the management of ICT related risks is aligned with the Municipality's overall risk tolerance.

Risk Categories

Each Risk is to be categorised into a group to allow for the correct response. These categories are:

Strategic - Major issues that affect the long term performance of the ICT Department
Operational - Includes information security, project and ICT service continuity risks
Financial - Covers all ICT operational costs
People - Includes loss or unavailability of key staff, or absence of required skills and competences
Compliance - Includes contractual and regulatory compliance

Responsibilities

The Municipal Manager is responsible for ensuring that the Municipality's risk management framework meets the organisational as well as legislative requirements in terms of risk management.

The Municipal Risk and Audit Committee must assist the Municipal Manager in carrying out his/her Corporate Governance of ICT accountabilities and responsibilities.

The ICT Manager must ensure that the Risk Matrix Table is updated on a regular basis to ensure that the management of ICT related risks is aligned with the Municipality's overall risk tolerance.

COMMENCEMENT OF THE POLICY

The policy will come into effect on the date signed by ICT Governance Champion

INTERPRETATION OF THE POLICY

All words contained in this policy shall have the ordinary meaning attached thereto, unless the definition or context indicates otherwise.
Any dispute on interpretation of this policy shall be declared in writing by any party concerned.
The Municipal Manager shall give a final interpretation of this policy in case of written dispute.
If the party concerned is not satisfied with the interpretation, a dispute may then be pursued with the South African Local Government Bargaining Council.

PERMANENT/TEMPORAL WAIVER OR SUSPENSION OF THE POLICY

This policy may be partly or wholly waived or suspended by the ICT Governance Champion on temporary or permanent basis however the Municipal Manager/Council may under circumstances of emergency temporarily waive this policy subject to reporting of such waiver or suspension to Council

COMPLIANCE AND ENFORCEMENT

Senior management is required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy.

Failure to comply with this policy may result in disciplinary action, which may include termination of employment.

Any conduct that interferes with the normal and proper operation of the municipality's IT systems, which adversely affects the ability of other users to use those IT systems, or which is harmful or offensive to other users, shall constitute violation of approved IT policies.

The municipality management reserves the right to revoke the privileges of any user at any time.

AMENDMENT AND/OR ABOLITION OF THIS POLICY

This policy may be amended or repealed by ICT Governance Champion /Council as it may deem necessary.

DOCUMENT OWNER AND APPROVAL

The Municipality is the owner of this document. The Executive Management of the Municipality is responsible for ensuring that this policy document is reviewed regularly to ensure that it remains relevant to the organisation.

This document was approved by the Executive Management and is issued on a version controlled basis under the signature of the ICT Governance Champion.

Every page of this document must also be initialled by the Governance Champion.