



**DR NKOSAZANA DLAMINI ZUMA LOCAL
MUNICIPALITY**

**ICT RISK MANAGEMENT
FRAMEWORK**

DR NDZLM ICT RISK MANAGEMENT FRAMEWORK

Document Control

Document Details

Document Name	RISK MANAGEMENT FRAMEWORK
Document Status	Approved
Version Number	1
Version Date	
Author	DR NDZLM Council

Review Control

Version	Status	Date	Name	Revision Description
1.0	Approved		Council	Annual reviewal

DR NDZLM ICT RISK MANAGEMENT FRAMEWORK

Table of Contents

Document Control.....	2
Table of Contents.....	3
1. INTRODUCTION.....	4
1.1. PURPOSE.....	5
1.2. TARGET AUDIENCE	5
2. RISK ASSESSMENT METHODOLOGY	6
2.1. ASSET IDENTIFICATION	6
2.2. THREAT IDENTIFICATION	7
2.3. VULNERABILITY IDENTIFICATION	10
2.4. CONTROL ANALYSIS	11
2.4.1. CONTROL METHODS	11
2.4.2. CONTROL CATEGORIES	11
2.4.3. RISK ASSESSMENT	12
2.4.4. PROBABILITY DETERMINATION.....	13
2.4.5. IMPACT DETERMINATION.....	14
Notes:.....	18
2.4.6. COMBINED RISK SCORE.....	19
2.5. RISK ACCEPTANCE CRITERIA.....	19
3. RISK TREATMENT.....	21
3.1. METHODS OF HANDLING THE RISK	21
4. APPENDIX A – LIST OF THREATS & VULNERABILITIES.....	32
4.1. THREATS.....	33
4.2. VULNERABILITIES	34
5. COMMENCEMENT OF THIS POLICY	35
6. INTERPRETATION OF THIS POLICY	35
7. PERMANENT/TEMPORARY WAIVER OR SUSPENSION OF THIS POLICY	35
8. AMENDMENT AND/OR ABOLITION OF THIS POLICY	36
9. COMPLIANCE AND ENFORCEMENT.....	36

1. INTRODUCTION

The mandate for Risk Management under South African legislation is established in Section 62 of the Municipal Finance Management Act (MFMA) No. 56 of 2003 and the Treasury Regulation Section 3.2, which stipulate the need for an effective, transparent risk management process and risk audit in compliance with the legislation.

The Accounting Officer has committed the Municipality to a risk management process aligned with good corporate governance principles, as supported by Section 38 of the Public Finance Management Act (PFMA), Act 1 of 1999 as amended.

According to Section 38(a) of PFMA, the Accounting Officer must ensure that the department has and maintains effective, efficient, and transparent systems of financial and risk management and internal control.

In line with the implementation of the Department of Public Service and Administration's (DPSA) Corporate Governance of Information and Communication Technology Policy Framework (CGICTPF), certain ICT processes have been selected from the Control Objectives for Information and Related Technology (COBIT) 5 framework for implementation by the Municipality, one of which is APO12: Manage Risk.

COBIT provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise ICT. COBIT 5 highlights the following practices in APO12 for managing ICT-related risks:

- a) Collect data:** Identify and collect relevant data to enable effective ICT-related risk identification, analysis, and reporting.
- b) Analyse risk:** Develop useful information to support risk decisions that take into account the business relevance of risk factors.
- c) Maintain a risk profile:** Maintain an inventory of known risks and risk attributes (including expected frequency, potential impact, and disposition) related to ICT resources, capabilities, and current control activities.
- d) Articulate risk:** Provide information on the current state of ICT-related exposures and opportunities in a timely manner to all required stakeholders for appropriate response.
- e) Manage risk:** Manage opportunities to reduce risk to an acceptable level as a portfolio.
- f) Respond to risk:** Respond in a timely manner with effective measures to limit the magnitude of loss from ICT-related events.

DR NDZLM ICT RISK MANAGEMENT FRAMEWORK

In addition, ISACA published the Risk IT Framework, which provides a set of good practices and a framework for enterprises to identify, govern, and manage ICT-related risks.

1.1. PURPOSE

The purpose of this Framework document is to provide guidance for conducting risk assessments of the Dr Nkosazana Dlamini Zuma Municipality's ICT. Risk assessments are part of an overall risk management process providing political leadership and senior management with the information needed to determine appropriate courses of action in response to identified risks.

This document provides guidance for carrying out each step in the risk assessment process (i.e., preparing for the assessment, conducting the assessment, communicating the results of the assessment, and maintaining the assessment) and how risk assessments and other organizational risk management processes complement and inform each other.

1.2. TARGET AUDIENCE

This publication is intended to serve a diverse group of risk management professionals including:

- Individuals with oversight responsibilities for risk assessment (e.g., Municipality Risk Management Committee).
- Individuals responsible for conducting organizational missions/business functions (e.g., Information owners, authorizing officials).
- Individuals responsible for acquiring information technology products, services, or information systems (e.g., acquisition officials, procurement officers, contracting officers).
- Individuals with information system/security design, development, and implementation responsibilities (e.g., program managers, enterprise architects, information security architects, information system/security engineers, information systems integrators).
- Individuals with information security oversight and operational responsibilities (e.g., Chief Information Officers, Senior Information Security Officers, Information Security Managers, Information System Owners, common Control Providers).

DR NDZLM ICT RISK MANAGEMENT FRAMEWORK

- Individuals with information security/risk assessment and monitoring responsibilities (e.g., system evaluators, penetration testers, security control assessors, risk assessors, independent verifiers/validators, inspectors general, auditors).

2. RISK ASSESSMENT METHODOLOGY

The Dr Nkosazana Dlamini Zuma Municipality should use risk assessments to determine the extent of potential threats and the risks associated with information assets. The output of this process helps identify appropriate controls for reducing or eliminating risks through the risk mitigation process.

Risk assessment exercises must be revised at least annually (or whenever any significant change occurs in the organization) by the Information Security Officer. All newly identified threats and vulnerabilities should be considered for treatment, and previously identified risks should be revisited to assess whether the applied controls are sufficient or need further treatment.

2.1 ASSET IDENTIFICATION

This document proposes a qualitative risk analysis model for assessing and maintaining the risk framework. The risk management team should comprise individuals from various groups within the organization. Representatives from these groups should work together to identify the assets within their teams that form the information asset list. This list identifies the various assets, their categories, and their locations.

Asset inventory exists in different forms, and those who hold this information are known as information asset owners. This can include:

- Information/Data assets
- Technology assets
- People assets
- Service assets

All information assets of the organization should be identified and documented. Once identified, assets are labelled according to predefined criteria (Information Labelling and Handling Procedure should be established by the organization).

DR NDZLM ICT RISK MANAGEMENT FRAMEWORK

Every information asset should have an owner or custodian. From a risk management perspective, the asset owner will be considered the risk owner and will be responsible for taking appropriate actions and adopting effective controls to lower the risk.

The owner and custodian of each asset are maintained in respective asset inventories. From a risk management perspective, the asset owner will be considered the risk owner and will be responsible for taking appropriate actions and adopting effective controls to lower the risk.

2.2. THREAT IDENTIFICATION

A threat represents the potential for a particular threat source to successfully exploit a vulnerability in an ICT system, either accidentally or intentionally. A threat source can be:

1. An intentional action aimed at exploiting a vulnerability, or
2. An accidental situation that triggers a vulnerability.

A vulnerability is a weakness in the system that can be either accidentally triggered or intentionally exploited. There is no risk from a threat source if there are no vulnerabilities present. Determining the likelihood of a threat involves considering threat sources, potential vulnerabilities, and existing controls.

2.2.1. Threat-source identification

The goal of this step is to identify potential threat sources and compile a threat statement listing those applicable to the information assets of Dr Nkosazana Dlamini Zuma Local Municipality.

A threat source is any circumstance or event with the potential to cause harm to an information asset. Common threat sources include natural events, human actions, and environmental conditions. For instance, even though the municipality might not be prone to natural floods, a burst pipe could still cause significant damage to IT assets.

Human threats can be intentional, such as deliberate attacks by malicious individuals or disgruntled employees, or unintentional, such as negligence and errors.

DR NDZLM ICT RISK MANAGEMENT FRAMEWORK

Common Threat-sources:

- **Natural Threats:** - Floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other such events.
- **Human Threats:** - Unintentional acts (e.g., data entry errors) or deliberate actions (e.g., network attacks, malware).
- **Environmental Threats:** - Long-term power failure, pollution, chemicals, liquid leakage.

2.2.2. 2.2 Motivation and Threat Actions

Motivation and the resources for carrying out an attack make humans potentially dangerous threat sources. Table 1 presents an overview of many common human threats, their possible motivations, and the methods or threat actions by which they might carry out an attack.

This information will be useful for the organization studying its human threat environment and customizing its human threat statements. Reviews of the history of system break-ins, security violation reports, incident reports, and interviews with system administrators, help desk personnel, and the user community during information gathering will help identify human threat sources that have the potential to harm an ICT system and its data where a vulnerability exists.

Table 1 –Threat-source and their motivations.

THREAT-SOURCE	MOTIVATION	THREAT ACTIONS
Hacker, Cracker	Challenge Ego Rebellion	▪ Hacking ▪ Social Engineering ▪ System intrusion, break-ins ▪ Unauthorised system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorised data alteration	▪ Computer crime (e.g., cyber stalking) ▪ Fraudulent act (e.g., replay impersonation, interception) ▪ Information bribery ▪ Spoofing ▪ System intrusion
Terrorist	Blackmail	▪ Bomb/Terrorism

DR NDZLM ICT RISK MANAGEMENT FRAMEWORK

	Destruction Exploitation Revenge	▪ Information warfare ▪ System attack (e.g. distributed denial of service) ▪ System penetration ▪ System tempering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorised system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g. data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g. virus, logic, bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorised system access

An estimate of the motivation, resources, and capabilities that may be required to carry out a successful attack should be developed after the potential threat-sources have been identified, in order to determine the likelihood of a threat's exercising a system vulnerability.

DR NDZLM ICT RISK MANAGEMENT FRAMEWORK

The threat statement, or the list of potential threat-sources, should be tailored to the individual organisation and its processing environment (e.g. end-user computing habits). In general, information on natural threats (e.g., floods, earthquakes, storms) should be readily available.

Output: A threat statement containing a list of threat-sources that could exploit system vulnerabilities.

2.3. VULNERABILITY IDENTIFICATION

Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

The analysis of the threat to an Information Asset must include an analysis of the vulnerability associated with the system environment. 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.

Table 2 – Vulnerabilities and Threats.

VULNERABILITY	THREAT- SOURCE	THREAT ACTION
Unremoved system IDs of terminated employees	Terminated employees	Unauthorized network access
Inbound telnet allowed; guest ID enabled	Hackers, terminated employees	Unauthorized system access
Unpatched security flaws	Hackers, disgruntled employees	Unauthorized access to sensitive files
Inadequate fire suppression in data centre.	Fire, negligence	Damage from water sprinklers

Output: A list of the system vulnerabilities (observations) that could be exercised by the potential threat-sources.

2.4. CONTROL ANALYSIS

The goal of this step is to analyse the controls that have been implemented or are planned for implementation by the organization to minimize or eliminate the likelihood (or probability) of a threat's exercising a system vulnerability.

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment, the implementation of current or planned controls must be considered.

For example, a vulnerability (e.g., system or procedural weakness) might not be exercised or the likelihood may be low if there is a low level of threat-source interest or capability or if there are effective security controls that can eliminate or reduce the magnitude of harm.

2.4.1. CONTROL METHODS

Security controls encompasses the use of technical and nontechnical methods. Technical controls are safeguards that are incorporated into computer, software, or firmware (e.g. access control mechanisms, identification and authentication mechanisms, encryption methods, intrusion detection software). Nontechnical controls are management and operational controls, such as security policies; operational procedures; and personnel, physical, and environmental security.

2.4.2. CONTROL CATEGORIES

The control categories for both technical and nontechnical control methods can be further classified as either preventive or detective. These two subcategories are explained as follows:

- **PREVENTIVE CONTROLS:** inhibit attempts to violate security policy and include such controls as success control enforcement, encryption, and authentication.
- **DETECTIVE CONTROLS:** warn of violations or attempted violations of security policy and include such controls as audit trails, intrusion detection methods, and checksums.

DR NDZLM ICT RISK MANAGEMENT FRAMEWORK

The implementation of such controls during the risk mitigation process is the direct result of the identification of deficiencies in current or planned controls during the risk assessment process. (E.g. controls are not in place or controls are not properly implemented).

Output: A list of current or planned controls used for the ICT systems to mitigate the likelihood of vulnerabilities being exercised and reduce the impact of such adverse events.

2.4.3. RISK ASSESSMENT

The adverse impact of a security event can be described in terms of loss or degradation of any, or combination of any, of the following three security goals: integrity, availability and confidentiality. The following list provides a brief description of each security goal and the consequence (or impact) of its not being met:

- **LOSS OF 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 ICT System by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an ICT system.

- **LOSS OF AVAILABILITY**

If a mission-critical ICT System is unavailable to its end users, the organisation's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end user's performance of their functions in supporting the organisation's mission.

- **LOSS OF CONFIDENTIALITY**

System and data confidentiality refers to the protection of information from unauthorised disclosure. The impact of unauthorised disclosure of confidential information can range from the jeopardising of national security to the disclosure of information under the Access to Information Act, Protection of Personal Information bill, Protection of

DR NDZLM ICT RISK MANAGEMENT FRAMEWORK

State Information Bill Act 2010, Protection of Information Act and Protection of Personal Information Act 4 of 2013. Unauthorised, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organisation.

Risks to information assets are assessed for breach of Confidentiality, integrity, and availability first, and then the combined risk is calculated using the formula defined in this section below.

Confidentiality Risk = Impact of Confidentiality % *Probability of Confidentiality%

Availability Risk = Impact of availability % *Probability of Availability %

Integrity Risk = Impact of Integrity % * Probability of Integrity.

2.4.4. PROBABILITY DETERMINATION

To derive probability rating that a potential vulnerability may be exercised within the construct of the associated threat environment, the following governing factors must be considered:

- Threat – source motivation and capability
- Nature of the vulnerability
- Existence and effectiveness of current controls

The probability that a potential vulnerability could be exercised by a given threat-source can be described as a very high, high, medium, low, or very low. Table below describes these five levels:

Table 3 – Probability of Occurrence (breach of C, I, A)

RATING	DESCRIPTION	PROBABILITY OF OCCURRENCE
1	Rare	Highly unlikely, but it may occur in exceptional circumstances. It could happen, probably never will.
2	Unlikely	Not expected, but there's slight possibility it may occur at some time.
3	possible	The event might occur at some time as there is a history of casual occurrence at the similar institutions.

DR NDZLM ICT RISK MANAGEMENT FRAMEWORK

4	Likely	There is a strong possibility the event will occur as there is a history of frequent occurrence at similar institutions.
5	Almost Certain	Very likely. The event is expected to occur in most circumstances as there is a history of regular occurrence at similar institutions.

2.4.5. IMPACT DETERMINATION

The adverse impact of the loss of confidentiality, integrity, and availability of the information asset, resulting from exploitation of a vulnerability by a threat, is determined based on the sensitivity of the information asset and the level of protection required. The information asset owners are the ones responsible for determining the impact level for their information assets.

The table below provides description of impact at the scale of 1 to 5 (with appropriate ratings) and is described from five different perspectives (financial Impact Client & Staff Ratings, Health & Safety, Business interruption, Reputation & Image, and Corporate Objectives).

DR NDZLM ICT RISK MANAGEMENT FRAMEWORK

Table 4 –Impact of breach of C, I, A

RATING	DESCRIPTION	FINANCIAL IMPACT	CLIENT & STAFF, HEALTH & SAFETY	BUSINESS INTERRUPTION	REPUTATION & IMAGE	CORPORATE OBJECTIVES
1	Insignificant	Minimal financial loss; less than R 1,000,000	No of minor personal injury; first aid needed but no days lost	Negligible; Critical systems unavailable for less than one hour	Negligible impact	Resolved in day –to– day management
2	minor	R 1,000,000 to R 5,000,000 not covered by insurance	Minor injury; Medical treatment & some days lost	Inconvenient; Critical systems unavailable for several hours.	Adverse local media coverage only	Minor Impact
3	Moderate	R 5,000,000 to R 20,000,000 not covered by insurance	Injury; hospitalisation	Client dissatisfaction; Critical Systems	Adverse capital City	Significant impact
4	Major	R 20,000,000 to R 50,000,000 not covered by insurance	Single death &/ long – term illness or multiple serious injuries	Critical Systems unavailable for 1 day or a series of prolonged outages	Adverse and extended national media coverage	Major impact

DR NDZLM ICT RISK MANAGEMENT FRAMEWORK

5	Catastrophic	R Above 50,000,000	Fatality(ies) or permanent disability or ill- health	Critical unavailable for more than a day (at a crucial time)	Systems for more government inquiry	Demand for	Disastrous impact

Notes:

- Financial Impact:** The amounts should be calibrated to reflect the financial realities and budget of Dr Nkosazana Dlamini Zuma Local Municipality. The values provided are indicative and should be adjusted according to local context.
- Client & Staff, Health & Safety:** Reflects the severity of impact on health and safety ranging from minor injuries to fatalities.
- Business Interruption:** The duration of critical system unavailability and its impact on operations.
- Reputation & Image:** The level of media coverage and public perception.
- Corporate Objectives:** The extent to which organizational goals and operations are affected.

Adjustments should be made in consultation with financial and risk management experts within the municipality to ensure they accurately reflect the local context and risk tolerance.

DR NDZLM ICT RISK MANAGEMENT FRAMEWORK

Thus, risk Score (for C, I, and A) may be between 1 (minimum value) and 5 (Maximum value).

Business Impact = 1 to 5

Likelihood = 1 to 5

It is important to calculate the Risk Score as it helps in prioritizing the treatment of Risk. If we do a Risk treatment on assets that has a low Risk Score, the cost to mitigate Risk on those assets might be much higher than the loss it could cause to the business.

Table 5 – Risk Impact Matrix

		IMPACT				
		1	2	3	4	5
LIKELIHOOD	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20
	5	5	10	15	20	25

DR NDZLM ICT RISK MANAGEMENT FRAMEWORK

Table 6 – Risk Impact Definitions

QUALITATIVE VALUES	SEMI- QUALITATIVE VALUES	DESCRIPTION
Very High	21 -25	Very High risk means that the threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the nation.
High	16 -20	High risk means that a threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the nation.
Moderate	10- 15	Moderate risk means that a threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the nation.
Low	6 - 9	Low risk means that a threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the nation.
Very Low	1 - 5	Very low risk means that a threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals, other organizations, or the nation.

Notes:

1. **Qualitative Values:** These are the descriptive terms used to convey the level of risk.
2. **Semi-Qualitative Values:** These numerical ranges are used to quantify the qualitative assessments, providing a bridge between qualitative and quantitative risk assessment.
3. **Description:** Detailed explanation of what each risk level means in terms of its potential impact on various aspects of the organization and beyond.

DR NDZLM ICT RISK MANAGEMENT FRAMEWORK

This table helps in standardizing the risk assessment process, ensuring that all stakeholders have a common understanding of the different levels of risk and their potential impacts.

2.4.6. COMBINED RISK SCORE

The Combined Risk (CR) is not a general average based on confidentiality (C), integrity (I) and Availability (A) values, but rather a weighted average where all other conditions from the impact assessment are taken into account.

When you need to find a value for the Combined Risk, one would typically choose between:

- 1) Average
- 2) Worst Case

However, in cases where only one value differs greatly from the other, the average will hide the deviated value, and worst case will become very high. We have therefore chosen to use both average and worst case

Use the following formula to calculate the CR.

$$\text{Combined Risk} = (\text{Average} + \text{Worst Case}) / 2$$

Where;

Average = (Confidentiality Risk + Integrity Risk + Availability Risk) /3

Worst Case = Highest Risk value among Confidentiality Risk, Integrity Risk, and Availability Risk

2.5. RISK ACCEPTANCE CRITERIA

Dr Nkosazana Dlamini Zuma Local Municipality (NDZLM) adopts a risk management framework that categorizes risks based on their assessed value. The criteria for risk acceptance within the municipality are as follows:

Risk Acceptance Threshold:

- **Accepted Risks:** NDZLM management will accept risks that have a value of nine (9) or less. These risks are considered manageable and within the municipality's capacity to handle without significant disruption or adverse impact.

DR NDZLM ICT RISK MANAGEMENT FRAMEWORK

- **Action Required for Higher Risks:** Any risk with a value above nine (9) will be subject to further review. Such risks will need to be addressed as deviations and require explicit management action. NDZLM management must either:
 - a. Accept the risk formally as a deviation, recognizing its potential impact and the rationale for acceptance.
 - b. Implement additional controls or mitigation measures to reduce the risk value to nine (9) or below.

Risk Review and Mitigation Process:

1. **Identification and Assessment:** Risks are identified and assessed using the established risk assessment framework, assigning qualitative and semi-qualitative values to determine the risk level.
2. **Review of Risks Above Threshold:** Risks scoring above the threshold value of nine (9) are escalated to the management level for detailed evaluation.
3. **Decision Making:**
 - **Risk Acceptance:** Management may accept the risk if it is deemed that the potential benefits outweigh the costs of further mitigation, or if the risk is unavoidable and within acceptable limits.
 - **Risk Mitigation:** If the risk is unacceptable, management will devise and implement appropriate measures to mitigate the risk. This may include enhancing existing controls, implementing new controls, allocating additional resources to manage the risk.
4. **Documentation and Monitoring:** All decisions regarding risk acceptance or mitigation are documented, including the justification for accepting risks above the threshold. Regular monitoring and reviews are conducted to ensure the effectiveness of the risk management strategies and to re-evaluate risks as necessary.
5. **Continuous Improvement:** NDZLM is committed to continuous improvement in its risk management practices. Lessons learned from risk management activities are used to refine and enhance the risk management framework and criteria.

Alignment with Legislation and Good Corporate Governance:

- **Compliance with South African Legislation:** NDZLM's risk management practices comply with relevant South African legislation, including the Protection of Personal Information Act (POPIA), Municipal Finance Management Act (MFMA), and other applicable laws and regulations.

DR NDZLM ICT RISK MANAGEMENT FRAMEWORK

- **Adherence to Good Corporate Governance:** NDZLM follows principles of good corporate governance as outlined in frameworks such as the King IV Report on Corporate Governance. This includes ensuring accountability, transparency, and integrity in all risk management activities.

Table 7 – Risk Acceptance Range

RISK CATEGORY	RISK RANGE
Very Low	1 to 5
Low	6 to 9
Medium	10 to 15
High	16 - 20
Very High	21 - 25

3. RISK TREATMENT

The ICT Risk Treatment Plan for Dr Nkosazana Dlamini Zuma Local Municipality (NDZLM) outlines the strategies and measures to address identified risks effectively. The treatment plan is based on the comprehensive risk analysis conducted, which highlights areas for improvement and guides the selection of appropriate risk treatment options. The plan ensures a holistic approach to managing risks throughout their lifecycle, documented within the risk assessment matrix.

3.1. METHODS OF HANDLING THE RISK

3.1.1. RISK MITIGATION

Risk mitigation involves implementing controls and measures to minimize the adverse impact of threats on ICT assets. The objective is to reduce the likelihood of threats materializing and limit the potential damage should they occur. The following strategies outline how Dr Nkosazana Dlamini Zuma Local Municipality (NDZLM) can effectively mitigate ICT risks:

3.1.1.1. Implementing Technical Controls

- **Anti-Virus and Anti-Malware Solutions:** Deploy comprehensive anti-virus and anti-malware software across all endpoints and servers. Ensure that virus definitions and software are regularly updated to protect against known and emerging threats.
- **Firewalls and Intrusion Detection Systems (IDS):** Install and configure firewalls to monitor and control incoming and outgoing network traffic based on predetermined security rules. Implement IDS to detect and alert on potential intrusions.
- **Regular Software Updates and Patching:** Establish a routine schedule for updating and patching all software, operating systems, and applications. This minimizes vulnerabilities that could be exploited by attackers.
- **Data Encryption:** Use encryption technologies to protect sensitive data both at rest and in transit. This ensures that even if data is intercepted or accessed without authorization, it remains unreadable and secure.
- **Access Controls:** Implement strict access controls to limit who can access ICT systems and data. Use multi-factor authentication (MFA) and role-based access controls (RBAC) to enhance security.

3.1.1.2. Administrative Controls

Policy Development and Enforcement: Develop comprehensive ICT policies that cover acceptable use, data protection, incident response, and other critical areas. Ensure these policies are enforced and regularly reviewed.

Training and Awareness Programs: Conduct regular training sessions for staff to raise awareness about cybersecurity threats and best practices. This includes phishing simulations, password management, and social engineering awareness.

Incident Response Plan: Develop and maintain an incident response plan that outlines the steps to be taken in the event of a security breach. Ensure all relevant personnel are familiar with their roles and responsibilities during an incident.

3.1.1.3. Physical Controls

Secure Physical Access: Implement physical security measures such as biometric access controls, security guards, surveillance cameras, and secure entry points to protect ICT infrastructure.

Environmental Controls: Ensure that server rooms and data centres are equipped with environmental controls like fire suppression systems, climate control, and uninterruptible power supplies (UPS) to protect against physical and environmental threats.

3.1.1.4. Data Management and Backup

- **Regular Backups:** Perform regular backups of all critical data. Store backups in multiple locations, including offsite or cloud storage, to ensure data availability in case of a disaster.
- **Backup Testing:** Regularly test backups to ensure that data can be restored accurately and quickly. This practice verifies the integrity of backups and the effectiveness of the backup process.

3.1.1.5. Monitoring and Evaluation

- **Continuous Monitoring:** Implement continuous monitoring solutions to detect and respond to security incidents in real-time. Use security information and event management (SIEM) systems to collect and analyse security data.
- **Regular Audits and Assessments:** Conduct regular security audits and assessments to identify vulnerabilities and ensure compliance with policies and regulations. Use the findings to improve security measures continuously.

3.1.1.6. Compliance and Governance

- **Compliance with Legislation:** Ensure that all ICT risk mitigation efforts comply with relevant South African laws and regulations, such as the Protection of Personal Information Act (POPIA) and the Municipal Finance Management Act (MFMA).
- **Good Corporate Governance:** Adhere to principles of good corporate governance, such as those outlined in the King IV Report on Corporate Governance. This includes maintaining transparency, accountability, and ethical behaviour in all ICT operations.

3.1.2. RISK TRANSFER

3.1.2. ICT Risk Transfer

- **Risk transfer** involves shifting the potential financial consequences and management responsibilities of specific ICT risks from Dr Nkosazana Dlamini Zuma Local Municipality (NDZLM) to another party. This can be achieved through various means such as purchasing insurance or outsourcing services, ensuring that the municipality can mitigate the impact of ICT-related incidents on its operations and resources.

3.1.2.1. Insurance Policies

- **Cyber Liability Insurance:** Obtain comprehensive cyber liability insurance to cover financial losses stemming from cyber incidents such as data breaches, ransomware attacks, and system outages. This insurance should cover legal fees, regulatory fines, notification costs, and recovery expenses.
- **Data Breach Insurance:** Secure data breach insurance to specifically address the costs associated with the loss or theft of sensitive data. Coverage should include expenses related to notifying affected individuals, public relations efforts, legal defence and credit monitoring services for impacted citizens.

3.1.2.2. Outsourcing and Managed Services

- **Managed Security Services:** Engage with reputable managed security service providers (MSSPs) to handle key aspects of NDZLM's cybersecurity operations. This includes continuous network monitoring, threat detection, incident response, and vulnerability management. Outsourcing these services transfers some of the risk to the MSSPs, who have specialized expertise and resources.
- **Cloud Service Providers:** Utilize cloud service providers (CSPs) that offer robust security measures and compliance with relevant regulations. Ensure service level agreements (SLAs) include provisions for data protection, regular backups, disaster recovery, and liability in case of security breaches.

DR NDZLM ICT RISK MANAGEMENT FRAMEWORK

3.1.2.3. Contractual Risk Transfer

- **Third-Party Contracts:** When entering into contracts with third-party vendors and service providers, include clauses that require them to maintain appropriate security measures and to indemnify NDZLM against any breaches that occur due to their negligence. Vendors should also have their own cybersecurity insurance.
- **Maintenance Contracts (MCs):** Establish maintenance contracts with third-party vendors for critical ICT infrastructure. These contracts should ensure that the vendors provide timely support and replacement parts, thereby minimizing downtime and transferring the risk of equipment failure to the vendors.

3.1.2.4. Strategic Partnerships

- **Public-Private Partnerships (PPPs):** Form strategic partnerships with private sector companies to share the risks associated with large-scale ICT projects. Such partnerships can provide access to advanced technologies and expertise while distributing the financial and operational risks between NDZLM and its partners.
- **Shared Services Agreements:** Enter into shared services agreements with other municipalities or government entities to leverage collective resources for ICT infrastructure and cybersecurity. This approach can reduce costs and distribute risks more evenly among the participating entities.

By implementing these risk transfer strategies, Dr Nkosazana Dlamini Zuma Local Municipality can effectively manage and mitigate the financial and operational impacts of ICT-related risks, ensuring continuity and resilience in its services.

3.1.3. RISK AVOIDANCE

To avoid the Risk by eliminating the Risk cause and / or consequence. If there is an old system (Windows 8 running some legacy / proprietary application), which cannot be patched for the current vulnerabilities, can be taken off the network to avoid risk of being compromised.

ICT Risk Avoidance Strategy for Dr Nkosazana Dlamini Zuma Local Municipality (NDZLM)

Removing Legacy Systems from the Network

- To mitigate the potential risks associated with outdated systems like Windows 8 running legacy or proprietary applications, NDZLM can adopt a proactive approach by implementing a risk avoidance strategy focused on removing these systems from the network. This approach aims to eliminate the risk cause and potential consequences associated with unsupported and vulnerable software.

1. System Assessment:

- Conduct a thorough assessment of all systems within NDZLM's network infrastructure to identify outdated operating systems, including Windows 8, and any associated legacy applications.

2. Risk Analysis:

- Perform a detailed risk analysis to evaluate the cybersecurity risks posed by running unsupported software. Consider factors such as the absence of security updates, increased susceptibility to malware, and potential non-compliance with regulatory standards.

-

3. Impact Analysis:

- Assess the potential impact on NDZLM's operations, data security, and service delivery in the event of a security breach or system compromise resulting from the continued use of outdated systems.

DR NDZLM ICT RISK MANAGEMENT FRAMEWORK

4. Decision Making:

- Based on the risk and impact analysis, make informed decisions regarding the removal of Windows 8 systems from the network. Consider factors such as the criticality of the legacy applications, feasibility of alternative solutions, and budgetary constraints.

5. Migration Planning:

- Develop a comprehensive migration plan to transition critical functions and data from the legacy Windows 8 systems to modern, supported platforms. This may involve upgrading to newer operating systems, virtualizing legacy applications, or seeking alternative software solutions.

6. Network Segmentation:

- Implement network segmentation to isolate the legacy systems from the rest of the network during the migration process. This reduces the attack surface and minimizes the risk of potential vulnerabilities affecting other network components.

7. Communication and Training:

- Communicate the rationale behind the decision to remove legacy systems from the network to relevant stakeholders within NDZLM. Provide comprehensive training and support to users impacted by the migration to ensure a seamless transition.

8. Monitoring and Compliance:

- Continuously monitor the network for any attempts to reintroduce unsupported systems or unauthorized devices. Enforce strict policies and procedures to maintain compliance with security best practices and regulatory requirements.
- By proactively removing outdated and vulnerable systems like Windows 8 from the network, NDZLM can significantly reduce the risk of cybersecurity incidents and enhance the overall resilience of its ICT infrastructure.

3.1.4. RISK ACCEPTANCE

Risk acceptance is a strategic decision-making process that acknowledges the limitations of risk mitigation efforts and allows NDZLM to manage unavoidable risks in a responsible and informed manner.

1. Risk Evaluation:

- Conduct thorough risk assessments to identify potential threats, vulnerabilities, and their associated impacts on NDZLM's ICT infrastructure and operations.

2. Risk Prioritization:

- Prioritize risks based on their likelihood, severity, and alignment with NDZLM's strategic objectives and operational priorities. Focus on risks that have the greatest potential impact on critical ICT assets and services

3. Risk Acceptance Criteria:

- Define clear criteria for accepting risks, considering factors such as feasibility, cost-effectiveness, regulatory compliance, and business continuity requirements. Establish thresholds for acceptable risk levels based on organizational tolerance and risk appetite.

4. Decision-Making Process:

- Engage relevant stakeholders, including senior management, IT professionals, and asset owners, in the risk acceptance decision-making process. Evaluate each risk scenario objectively and transparently, weighing the potential benefits against the associated risks.

5. Justification and Documentation:

- Document the rationale behind risk acceptance decisions, including any mitigating controls or alternative measures considered. Ensure that all decisions are justified based on a comprehensive analysis of risk factors and organizational constraints.

DR NDZLM ICT RISK MANAGEMENT FRAMEWORK

6. Management Approval:

- Seek approval from appropriate management authorities, such as executive leadership or steering committees, before formally accepting identified risks. Obtain consensus among stakeholders regarding the level of risk tolerance and the proposed risk acceptance strategy.

7. Periodic Review:

- Regularly review accepted risks to assess their ongoing relevance and effectiveness of existing controls. Update risk acceptance criteria as needed based on changing business requirements, technological advancements, or regulatory changes.

8. Communication and Transparency:

- Communicate accepted risks and associated mitigation strategies to relevant stakeholders, fostering transparency and accountability within NDZLM. Ensure that all parties understand their roles and responsibilities in managing accepted risks effectively.

9. Continuous Improvement:

- Foster a culture of continuous improvement by soliciting feedback from stakeholders and conducting post-implementation reviews of risk acceptance decisions. Identify opportunities for enhancing risk management processes and optimizing resource allocation.
- By adopting a systematic approach to risk acceptance, NDZLM can strike a balance between operational flexibility and risk mitigation, ensuring the resilience and sustainability of its ICT infrastructure in the face of evolving threats and challenges.

3.1.5. RESIDUAL RISK

Residual risk refers to the remaining level of risk after risk treatment measures have been implemented. NDZLM acknowledges that despite mitigation efforts, residual risks may still exist. Therefore, it's crucial to manage these residual risks effectively to maintain an acceptable level of risk exposure.

1. Identification of Residual Risks:

- After implementing risk treatment decisions, conduct a reassessment of all identified risks to determine the residual risk levels. Residual risks are those that remain above the acceptable threshold despite treatment measures.

2. Evaluation and Prioritization:

- Evaluate residual risks based on their likelihood, severity, and potential impact on NDZLM's ICT infrastructure and operations. Prioritize residual risks according to their significance and alignment with organizational objectives.

3. Management Review and Acceptance:

- Present residual risks to the management committee for review and acceptance. Management must objectively assess the residual risks and determine whether they are within acceptable tolerances or require further action.

4. Documentation and Approval:

- Document all accepted residual risks along with the rationale for acceptance. Ensure that management approval is obtained for each accepted residual risk. Maintain a comprehensive record of residual risk acceptance decisions for future reference and audit purposes.

5. Periodic Review and Reassessment:

- Regularly revisit residual risks during routine risk assessments or whenever a new threat is discovered. Update the status of residual risks based on changes in the threat landscape, technological advancements, or organizational priorities.

DR NDZLM ICT RISK MANAGEMENT FRAMEWORK

6. Mitigation Planning:

- Develop mitigation plans for residual risks that exceed acceptable thresholds or pose significant threats to NDZLM's operations. Implement additional controls or measures to reduce the residual risk to an acceptable level where feasible and cost-effective.

7. Continuous Monitoring and Improvement:

- Continuously monitor the effectiveness of residual risk management strategies and adjust them as necessary. Promote a culture of proactive risk management and continuous improvement within NDZLM to enhance resilience and adaptability.

8. Communication and Transparency:

- Communicate accepted residual risks and mitigation strategies to relevant stakeholders, ensuring transparency and accountability. Foster open dialogue and collaboration to facilitate effective risk management across the organization.
- By systematically addressing residual risks, NDZLM can enhance its ability to identify, assess, and respond to emerging threats, thereby safeguarding its ICT assets and supporting its mission-critical operations.

4. APPENDIX A – LIST OF THREATS & VULNERABILITIES

One of the initial planning steps in a risk management program is to generate a comprehensive list of sources of threats, risks, and events that might have an impact on the ability of the organisation to achieve its objectives as identified in the definition of scope and the framework. These events might prevent, degrade, delay or enhance the achievement of those objectives.

In general, a risk can be related to or characterised by:

- It's origin – e.g., threat agents such as hostile employees, employees not properly trained, competitors, governments, etc.
- A certain activity, event or incident (i.e., threat) e.g., unauthorised dissemination of confidential data, competitor deployment of a new marketing policy, new or revised data protection regulations, an extensive power failure.
- A specific reason for its occurrence - e.g., system design error, human intervention, prediction or failure to predict competitor activity.
- Protective mechanisms and controls (together with their possible lack of effectiveness) e.g., access, control and detection systems, policies, security training, market research and surveillance of market
- Time and place of occurrence – e.g., a flood in the computer room during extreme environmental conditions.

DR NDZLM ICT RISK MANAGEMENT FRAMEWORK

4.1. THREATS

THREATS

Access to the network by unauthorised person	Disclosure of information	Interruption of business processes
Bomb attack	Disclosure of passwords	Loss of electricity
Bomb threat	Eavesdropping	Malfunction of equipment
Breach of contractual relations	Embezzlement	Malicious code
Breach of Legislation	Errors in maintenance	Misuse of information systems
Compromising confidential information	Failure of communication links	Misuse of audit tools
Concealing user identification	Falsification of records	Pollution
Damage caused by a third party	Fire	Social engineering
Damages resulting from penetration testing	Flood	Software errors
Destruction of records	Fraud	Strike
Disaster (Human caused)	Industrial espionage	Terrorist attack
Disaster (Natural)	Information leakage	Theft
thunder stroke	Unintentional change of data in an information system	Unauthorised access to the information system
Unauthorised changes of records	Unauthorised installation of software	Unauthorised physical access
Unauthorised use copyright material	Unauthorised use of software	User error
Vandalism		

DR NDZLM ICT RISK MANAGEMENT FRAMEWORK

4.2. VULNERABILITIES

Default passwords not changed	Disposal of storage media without deleting data	Equipment sensitivity to moisture and contaminants
Equipment sensitivity to temperature	Inadequate cabling security	Inadequate capacity management
Inadequate classification of information	Inadequate control of physical access	Inadequate maintenance
Inadequate network management	Inadequate or irregular backup	Inadequate password management
Inadequate physical protection	Inadequate protection of cryptographic keys	Inadequate replacement of older equipment
Inadequate security awareness	Inadequate segregation of duties	Inadequate segregation of operational and testing facilities
Inadequate supervision of employees	Inadequate supervision of vendors	Inadequate training of employees
Incomplete specification for software development	Insufficient software testing	Lack of access control policy
Lack of clean desk and clear screen policy	Lack of control over the input and output data	Lack of internal documentation
Lack or poor implementation of internal Audit	Lack of policy for the use of cryptography	Lack of procedure for removing access rights upon termination of employment
Lack of protection of mobile equipment	Lack of redundancy	Lack of systems for identification and authentication
Lack of validation of the processed data	Location vulnerable to flooding	Poor selection of test data
Uncontrolled download from the internet	Uncontrolled use of information systems	Unmotivated employees

DR NDZLM ICT RISK MANAGEMENT FRAMEWORK

Unprotected public network connections	User right are not reviewed regularly.	
--	--	--

5. COMMENCEMENT OF THIS POLICY

This policy will come into effect on the date of adoption by the Council.

6. INTERPRETATION OF THIS POLICY

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

7. PERMANENT/TEMPORARY WAIVER OR SUSPENSION OF THIS POLICY

- 7.1. This policy may be partly or wholly waived or suspended by the Municipal Council on a temporary or permanent basis, after consultation with Management and Trade Unions.
- 7.2. Notwithstanding clause No. 10.1 the Municipal Manager may under circumstances of emergency temporarily waive or suspend this policy subject to reporting of such waiver or suspension to Council and Trade Unions.

DR NDZLM ICT RISK MANAGEMENT FRAMEWORK

8. AMENDMENT AND/OR ABOLITION OF THIS POLICY

This policy may be partly amended or repealed by the Council after consultation and interaction with Management and Trade Unions.

9. COMPLIANCE AND ENFORCEMENT

- 9.1. Violation of or non-compliance with this policy will give a just cause for disciplinary steps to be taken.
- 9.2. It will be the responsibility of all Managers, Supervisors, Executive Committee and Council to enforce compliance with this policy.

10. APPROVAL

Signature	Approved By:	Date
	SI Sonderu	28 May 2026