# ICT DISASTER RECOVERY BUSINESS IMPACT ANALYSIS

Council resolution: **ITEM 19/05/29/9.12**

## TABLE OF CONTENTS

### Document Identification

### Preparation

| Action | Name | Role / Function | Date |
|---|---|---|---|
| Prepared by: | Hendrik Matthews | Manager – Information Technology | 2019-04-23 |
| Reviewed/Approved by: | ICT Steering Committee | Chairperson | 2019-04-23 |

### Glossary of Abbreviations

| Abbreviation | Definition |
|---|---|
| BCMS | Business Continuity Management System |
| BC | Business Continuity |

| Abbreviation | Definition |
|---|---|
| DR | Disaster Recovery |
| DRP | Disaster Recovery Plan |
| HR | Human Resources |
| ICT | Information and Communication Technology |
| MTO | Maximum Tolerable Outage |
| RTO | Recovery Time Objective |
| RPO | Recovery Point Objective |
| RACI | Responsible, Accountable, Consulted, Informed |

## Glossary of Terminologies

| Terminology | Definition |
|---|---|
| Business case | A formal requirement in order for a specific business function to perform its required task, such as to implement a project initiative. |
| Line manager | Each department (HR, Finance, ICT, etc.) should have a manager employed to perform managerial tasks. |
| Main Site | Municipal Head Office and assumed in some case to be the location of the Municipality Main Data Centre |
| Maximum Tolerable Outage | The amount of time the identified critical business function may be unavailable before the Municipality is severely impacted. |
| Procurement | The external acquisition of services, assets and consumables, whether by outright purchase, hire, licensing or outsourcing. |
| Recovery Point Objective | The worst data loss that the Municipality is willing to accept. In other words, this is the point from which recovery of lost data must take place. |
| | |
| | |
| Service | A Service delivered to the municipality by ICT or by 3rd parties. Examples: email, Internet, printing. |
| Contract | An agreement (which may be verbal or in writing) entered into with the intention of creating legally binding consequences. The contract includes all annexures, schedules, etc., as well as any agreed amendments. |
| Incident | Typically impacts a specific service or server. Examples of Incidents include a compromised service resulting from a hacking attack or the partial loss of an office area due to a burst water pipe. |

| Terminology | Definition |
|---|---|
| Disaster | A significant or unusual Incident that has long-term implications. An example of a disaster would be the loss of a building due to a fire . |
| Disaster (formal definition as per The Disaster Management Act) | The Disaster Management Act (Act No. 57 of 2002) defines a disaster as a progressive or sudden, widespread or localised, natural or human-caused occurrence which:<br>• Causes or threatens to cause:<br>○ Death, injury and/or disease.<br>○ Damage to property, infrastructure and/or the environment.<br>○ Disruption of life, within the community.<br>• Is of a magnitude that exceeds the ability of those affected by the disaster to cope with its effects using only their own resources. |
| Test Plan | The DR Test Plan document provides guidance on the types, details, scheduling, effort and activity required for regular testing every year. |

## 1. INTRODUCTION

This document provides the Municipality with the information, procedures and templates required to conduct a business impact assessment (BIA) and vulnerability pertaining to key Municipal operations that are dependent on ICT systems.

The document supports the Municipality’s ICT Governance Policy and was developed with the legislative environment in mind, as well as to leverage internationally recognised ICT standards.

This document forms part of the Municipality’s ICT DR Policy.

## 2. LEGISLATION

The policy was drafted bearing in mind the legislative conditions, as well as to leverage internationally recognised ICT standards.

The following legislation, among others, were considered in the drafting of this policy:

- Constitution of the Republic of South Africa Act, Act No. 108 of 1996;
- Copyright Act, Act No. 98 of 1978;
- Electronic Communications and Transactions Act, Act No. 25 of 2002;
- Minimum Information Security Standards, as approved by Cabinet in 1996;
- Municipal Finance Management Act, Act No. 56 of 2003;
- Municipal Structures Act, Act No. 117 of 1998;
- Municipal Systems Act, Act No. 32, of 2000;
- National Archives and Record Service of South Africa Act, Act No. 43 of 1996;
- Promotion of Access to Information Act, Act No. 2 of 2000;
- Protection of Personal Information Act, Act No. 4 of 2013;
- The Disaster Management Act, Act No. 57 of 2002; Regulation of Interception of Communications Act, Act No. 70 of 2002; and
- Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005.

The following internationally recognised ICT standards were leveraged in the development of this policy:

- Western Cape Municipal Information and Communication Technology Governance Policy Framework, 2014;
- Control Objectives for Information Technology (COBIT) 5, 2012;
- ISO 27002:2013 Information technology — Security techniques — Code of practice for information security controls; and

King Code IV Principles

## 3. OBJECTIVE OF THE DR BUSINESS IMPACT ANALYSIS

The objective of this document is to conduct regular business impact assessments analysis of the Municipal operations. The business requirements for recovery of systems are tabulated and stated in technical terms (e.g.: MTO, RPO, RTO), categorised and summarised, so that Adequate solutions can be investigated for a successful ICT DR Plan in the event of a disaster.

The objectives of this document are to enable the following: Describe the business organisation, with particular focus on the functions and supporting ICT applications.

- Evaluate any key building features, vulnerabilities and observations.
- Describe the business disruption categories
- Specify the availability and recovery requirements for critical business functions and ICT systems.
- Analyse resource continuity requirements.
- Support a business continuity strategy that must be developed further into a BCMS in future years.

## 4. THE AIM OF THIS DR BUSINESS IMPACT ANALYSIS

The aim of this ICT Disaster Recovery Business Impact Analysis document is to assist the ICT Manager, Line Managers and duly authorised employees the municipality to conduct an effective analysis that might disrupt business operations, specifically within the context of protecting and recovering key supporting ICT systems.

This analysis enables the preparation of an effective ICT DR Plan, as well as upgrading or improving underlying applications and technology, for the recovery of ICT systems supporting the West Coast District Municipality.

## 5. SCOPE

This document covers the functional activities (pertaining to departments, divisions and key functions) of the employees of the West Coast District Municipality. Key employees from the Municipality, representing the various Municipal operations and functions, should be informed of this BIA document.

The following is not included in the scope of this document:

- Employees located outside of the West Coast District Municipality based offices
- External stakeholders

### 5.1 Associated ICT DR documents

This ICT Disaster Recovery Business Impact Analysis document resides in a broader ICT DR framework of five key documents as summarised below:

| Document | Summary |
|---|---|
| ICT DR Policy. | • Broad policy, principles, high level framework & obligations. |
| ICT Business & Impact Analysis. | • Business & Vulnerability Analysis; and<br>• Business Impact Assessment. |
| ICT DR Plan. | • Actionable Plan in event of Disaster incl. teams, processes & forms/templates. |
| Definition of ICT DR Architecture. | • Technical Assessments;<br>• Architecture(s) for Current Live & DR environment; and<br>• Service details. |
| ICT DR Test Plan. | • Tiered Test plan. |

**Table 1: ICT DR Framework documents**

## 6. ASSESSMENT PREPARATION

6.1 General

6.1.1 The ICT Manager must request the help of Line Managers, to populate Appendices A.1, A.2, A.3 which are tables pertaining to the organogram, building locations for all key Municipal departments, and the functions pertaining to each division or department Information must be obtained from each department within the West Coast District Municipality to ensure that a complete view of the recovery requirements is obtained for the ICT DRP Plan.:

- *Key* business functions
- *How often* the functions are performed
- What *applications* (if any) are used to perform the functions
- How *critical* is the function to the Municipality
- *Recovery requirements* for the functions
- Electronic and non-electronic *dependencies*
- Key resources requirements (out of scope/not related to ICT)

6.1.2 The ICT Manager must request assistance from the Line Managers and/or Application owners in order to get an updated and date-stamped tabular representation of all business *applications* (see Appendix A.4)

# 7. ASSESSMENT FRAMEWORK

## 7.1 Business disruption categories

There are an almost indefinite number of potential threats, with varying levels of likelihood that could result in a severe disruption to normal business operations. The table below summarises the threats into eight business disruption categories, and provides example scenarios for each, along with an indication of which plan it is applicable to.

| Disruption category | Example scenarios | Applies to |
|---|---|---|
| Loss of data services | Server failure, database corruption | • BCP/ ICT DRP |
| Loss of voice services | IPT failure, loss of telephone lines | |
| Loss of key dependencies | Power failure, water failure | |
| Loss of key staff | Resignation, illness | |
| Loss of vital non-electronic records | Fire, damage to files, historical archives | |
| Loss of precinct | Natural disaster, terrorism | |
| Loss of building | Fire, structural failure | |
| Denial of access to building | Labour unrest, localised disaster | |

# 8. BUSINESS IMPACT ANALYSIS

## 8.1 Loss of data services

The table below summarises the business analysis for loss of data services.

| Potential causes | Potential consequences |
|---|---|
| • Data/systems failure<br>• Inadequate resources (human and/or technological)<br>• Inadequate internal control systems<br>• Inadequate backup and archiving processes<br>• Security breaches (theft, vandalism, etc.)<br>• Virus/hacker /denial of service<br>• Power failure<br>• Air-conditioning failure<br>• Fire, flooding or structural failure<br>• Patch Management<br>• Antivirus and Firewall protection<br>• Inadequate password policy and control | • Loss of assets<br>• Loss of revenue<br>• Inability to provide services<br>• Client dissatisfaction<br>• Employee dissatisfaction<br>• Creation of liabilities<br>• Reputation risk<br>• Legal penalties<br>• Drain on resources<br>• Additional on-going costs |

| | |
|---|---|
| • Ineffective physical security measures | |
| **Control environment overview** | |
| **Existing control measures** | **Recommended additional control measures** |
| • Restricted access to computer rooms<br>• Access control into building, office and server rooms<br>• ICT system backups<br>• Offsite backups of some systems<br>• Uninterrupted power supplies (UPS), air-conditioners, smoke detectors<br>• Antivirus, intrusion detection and firewalls are implemented, updated, reviewed and monitored<br>• Manage and administrative systems<br>• Password protection on all computers | • Physical security controls in buildings need attention to ensure that unauthorised access is prevented<br>• Access must be properly logged<br>• Service level agreements need to be reviewed and implemented for all critical areas<br>• Regular tests of data recovery processes<br>• Automated fire suppression systems need to be implemented<br>• Environmental monitoring needs to be implemented<br>• Offsite storage and data replication for all systems<br>• Configuration and change management<br>• Generators must be installed for all sites<br>• Graceful shutdown must be implemented on critical systems to prevent corruption due to incorrect shutdown procedures |

## 8.2 Loss of voice services

The table below summarises the business analysis for loss of voice services.

| **Potential causes:** | **Potential consequences:** |
|---|---|
| • Inadequate resources (human and/or technological)<br>• Inadequate internal control systems<br>• Loss of server room<br>• PABX failure<br>• Carrier failure<br>• Power failure<br>• Cable theft | • Difficulty in providing services<br>• Client dissatisfaction<br>• Employee dissatisfaction<br>• Reputation risk<br>• Drain on resources<br>• Additional on-going costs |
| **Control environment overview** | |
| **Existing control measures:** | **Recommended additional control measures:** |
| • Limited access to PABX room<br>• Telephone Management Systems with buffers<br>• Service contract in place for all telephony equipment<br>• Battery backups | • Install generators to power equipment and servers<br>• Implement redundant telecommunication path<br>• Environmental monitoring for server room |

| | |
|---|---|
| • Air-conditioning in server room | |

## 8.3 Loss of key dependencies

The table below summarises the business analysis for loss of key dependencies.

| Potential causes | Potential consequences |
|---|---|
| • Inadequate supplier resources (human and/or technological)<br>• Inadequate internal control systems (supplier)<br>• Data/systems failure<br>• Breaches of security (supplier)<br>• Virus/hacker/denial of service<br>• Power failure<br>• Air-conditioning failure<br>• Fire<br>• Flooding<br>• Structural failure<br>• Unstable or Unavailable internet Access | • Loss of assets<br>• Inability to provide services<br>• Client dissatisfaction<br>• Manual control of lights, water, generators and cooling<br>• No monitoring of lights, water, generators and cooling<br>• Action by regulators<br>• Employer dissatisfaction<br>• Creation of liabilities<br>• Reputation risk<br>• Legal penalties<br>• Drain on resources<br>• Additional on-going costs |
| **Control environment overview** | |
| **Existing control measures** | **Recommended additional control measures** |
| • UPS battery backup<br>• Smoke detection and fire suppression systems are serviced regularly according to a service schedule<br>• Antivirus, intrusion detection and firewalls are implemented<br>• Restricted access to computer rooms<br>• Smoke detectors | • Combined business continuity planning and testing with key suppliers<br>• Generators need to be installed for all hosting facilities to ensure continuous supply of power<br>• Operating procedures and check-lists to reduce reliance on individuals and suppliers<br>• Service level agreements need to be reviewed and implemented<br>• Environmental monitoring systems need to be implemented<br>• Automated fire suppression system needs to be implemented<br>• Physical security controls need to be improved |

## 8.4 Loss of key staff

The table below summarises the business analysis for loss of key staff.

| **Potential causes** | **Potential consequences** |
|---|---|
| - Breaches of physical security<br>- Biological threat (e.g. Avian influenza)<br>- Injury or illness<br>- Resignation | - Loss of knowledge<br>- Reduced productivity<br>- Drain on resources<br>- Additional on-going costs |
| **Control environment overview** | |
| **Existing control measures** | **Recommended additional control measures** |
| - Detailed job descriptions and performance agreements (identify which teams, roles, ICT?)<br>- Good knowledge transfer between staff is happening – should be categorised.<br>- Security at main entrance and office entrances | *Note: Municipality should apply to both ICT staff and operations staff:*<br>- Succession planning for key staff<br>- Improve turnaround time to acquire resources<br>- Standard operating procedures to reduce reliance on individuals and suppliers<br>- Hiring of additional staff<br>- Outsourcing of some functions<br>- Documentation of all business processes<br>- Employee incentive schemes<br>- Additional staff training<br>- Standing agreement with recruitment agencies<br>- Security need to verify the identity of visitors |

## 8.5 Loss of vital non-electronic records

The table below summarises the business analysis for loss of vital non-electronic records.

| **Potential causes** | **Potential consequences** |
|---|---|
| - Natural disaster<br>- Fire<br>- Flood damage<br>- War or civil disturbance<br>- Terrorism<br>- Severe weather<br>- Structural failure<br>- Theft<br>- Employee negligence | - Loss of assets<br>- Inability to provide services<br>- Client dissatisfaction<br>- Action by regulators<br>- Employee dissatisfaction<br>- Creation of liabilities<br>- Reputation risk<br>- Legal penalties<br>- Drain on resources<br>- Additional on-going costs |
| **Control environment overview** | |
| **Existing control measures** | **Recommended additional control measures** |

| | |
|---|---|
| • Fire suppression. (E.g. hose reels, fire extinguishers & blankets)<br>• Offices are well maintained<br>• Security at main building entrance and office entrance<br>BC only<br>• File tracking system<br>• Filing room | • Automated fire suppression needs to be installed in critical areas<br>• Verification of visitor identities<br>• Electronic archiving system<br>• Non electronic copies to be made and kept offsite<br>• Offsite storage and backups for electronic archives<br>• Alternative business site to be established<br>*Pertaining to BC*:<br>• Fire marshals need to be identified and trained<br>• Fire resistant safe and filing areas need to be established<br>• Fire and smoke detection systems need to be implemented in all critical areas |

## 8.6 Loss of precinct

The table below summarises the business analysis for loss of precinct.

| **Potential causes** | **Potential consequences** |
|---|---|
| • Natural disasters<br>• Severe weather<br>• Fire<br>• Flood<br>• Biological threat (e.g. Avian Influenza)<br>• War or civil disturbance<br>• Terrorism | • Loss of assets<br>• Inability to provide services<br>• Client dissatisfaction<br>• Action by regulators<br>• Employee dissatisfaction<br>• Creation of liabilities<br>• Reputation risk<br>• Legal penalties<br>• Drain on resources<br>• Additional on-going costs |
| **Control environment overview** | |
| **Existing control measures** | **Recommended additional control measures** |
| • Fire and smoke detection systems<br>• Fire suppression. (E.g. Data centre and ICT wiring closets)<br>• Offsite Data Backup's (partial/tape) | • Remote connectivity to be made available to key staff<br>• Offsite storage and backups for electronic data<br>• Detailed ICT and system recovery procedures<br>• Replication of virtual servers to alternative sites<br>• Alternative business site to be established |

| | |
|---|---|
| | Typical BC controls:<br>• Fire marshals need to be identified and trained<br>• Fire resistant safe and filing areas need to be established |

## 8.7 Loss of building

The table below summarises the business analysis for loss of building.

| Potential causes | Potential consequences |
|---|---|
| • Natural disaster<br>• Fire<br>• Flood<br>• War or civil disturbance<br>• Terrorism<br>• Severe weather<br>• Structural failure | • Loss of assets<br>• Inability to provide services<br>• Client dissatisfaction<br>• Action by regulators<br>• Employee dissatisfaction<br>• Creation of liabilities<br>• Reputation risk<br>• Legal penalties<br>• Drain on resources<br>• Additional on-going costs |
| **Control environment overview** | |
| **Existing control measures** | **Recommended additional control measures** |
| • Offices are well maintained<br>• Access Control at main building entrance and office entrance<br>• Offsite storage for some systems | • Remote connectivity to be made available to key staff<br>• Fire and smoke detection systems need to be implemented in all areas<br>• Verification of visitor identities<br>• Offsite storage and backups for all electronic data<br>• Detailed ICT and system recovery procedures<br>• Replication of virtual servers to alternative sites<br>• Alternative business site to be established<br>BC specific controls<br>• Fire marshals need to be identified and trained<br>• Fire resistant safe and filing areas need to be established |

## 8.8 Denial of access to building

The table below summarises the business analysis for denial of access to building.

| Potential causes | Potential consequences |
|---|---|
| • Natural disaster<br>• Fire<br>• Flood<br>• Biological threat (e.g. Avian Influenza, Anthrax hoax)<br>• Chemical spill<br>• War or Civil disturbance<br>• Terrorism<br>• Severe weather<br>• Structural failure<br>• Industrial dispute | • Loss of assets<br>• Inability to provide services<br>• Client dissatisfaction<br>• Action by regulators<br>• Employee dissatisfaction<br>• Reputation risk<br>• Legal penalties<br>• Drain on resources<br>• Additional on-going costs |
| **Control environment overview** | |
| **Existing control measures** | **Recommended additional control measures** |
| • Fire and smoke detection systems<br>• Fire suppression. (E.g. Data centre and ICT wiring closets)<br>• Offices are well maintained. ICT office is well maintained<br>• Access Control at main building entrance and office entrance<br>• Offsite storage of some data | • Remote connectivity to be made available to key staff<br>• Verification of visitor identities<br>• Offsite storage and backups for all electronic data<br>• Detailed ICT and system recovery procedures<br>• Replication of virtual servers to alternative sites<br>• Alternative business site to be established<br>BC controls:<br>• Fire marshals need to be identified and trained<br>• Fire resistant safe and filing areas need to be established |

## 9. AVAILABILITY AND RECOVERY REQUIREMENTS

### 9.1 Critical business functions

The MTO is the amount of time the identified critical business function may be unavailable before the Municipality is severely impacted. The RPO is the worst data loss that the Municipality is willing to accept. In other words, this is the point from which recovery of lost data must take place. The MTO and RPO are based on a 24 hour day/ 7 day week allowed for recovery.

### 9.2 ICT recovery requirements

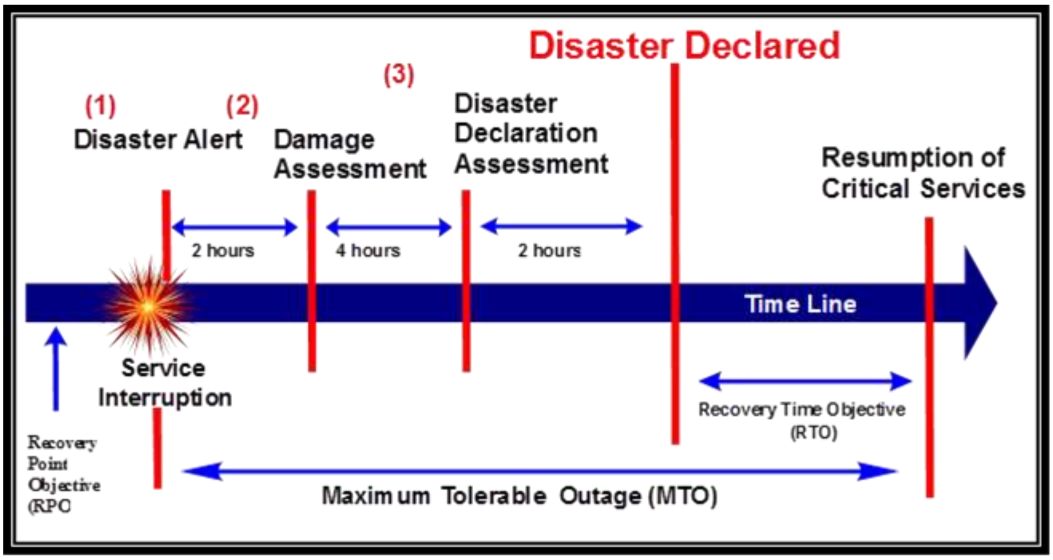
### 9.2.1 General Terms

The figure below depicts an example of ICT recovery requirements in terms of:

(1) Disaster alert: The time taken to alert Municipality that a potential disaster has occurred

(2) Evaluation/Damage assessment: The time taken to assess the damage of a potential disaster

(3) Disaster declaration assessment: The time taken to assess whether to declare an actual disaster situation


Disaster Declared
(1)
Disaster Alert
(2)
Damage Assessment
(3)
Disaster Declaration Assessment
Resumption of Critical Services
2 hours
4 hours
2 hours
Time Line
Service Interruption
Recovery Point Objective (RPO
Recovery Time Objective (RTO)
Maximum Tolerable Outage (MTO)

The recovery time objective (RTO) is the time taken to restore the infrastructure and hand it over to the business teams. The RTO is the difference between the MTO and the time required to declare a disaster.

For example:

- If the MTO for a system is 24 hours and it takes the Municipality 8 hours to declare a disaster, the RTO for that system is 16 hours.

### 9.2.2 Deriving the ICT Service Recovery requirements

The ICT service recovery requirements are derived by assessing the business systems (applications) and dependent technology that support the critical business functions (see Section 9.1). These are then mapped into the ICT recovery requirements table, and the recovery requirements (MTO, RPO and RTO), and dependencies are mapped to these ICT services

Note: The MTO, RTO and RPO are based on a 24 hour day allowable for recovery.

## 10. CONTINUITY RESOURCE ANALYSIS

This section assesses the employees, resources and applications required to ensure business continuity in the event of a disaster.

### 10.1 Applications required per Department

The table below summarises the core applications required for the departments

**Legend:**

| | |
|---|---|
| Required | ✓ |
| Not required | × |

| Division | ERP | Collaborator | CAPMAN | IGNITE | EUNOMIA |
|---|---|---|---|---|---|
| Office of the MM | ✓ | ✓ | × | ✓ | ✓ |
| Administration | × | ✓ | × | ✓ | ✓ |
| Technical Services | × | ✓ | × | ✓ | × |
| Human Resources | × | ✓ | ✓ | ✓ | × |
| Financial Services | ✓ | ✓ | × | ✓ | ✓ |

In addition to the core applications summarised in

**Table** 2 **all staff will require email, Internet and MS Office.**

### 10.1.1 Department: Office of Municipal Manager

SAMRAS
Collaborator
Capman
IGNITE
Eunomia

### 10.1.2 Department: Finance

SAMRAS
Collaborator
Capman
IGNITE
Eunomia

### 10.1.3 Department: Technical Services

SAMRAS
Collaborator
Capman
IGNITE
Eunomia

### 10.1.4 Department: Administration and Community Services

SAMRAS
Collaborator
IGNITE
Eunomia

## 11. BUSINESS CONTINUITY STRATEGY

The strategy provided is with regard to ICT provision of controls and DR capability, which can be implemented to support the business functions

| **Strategy recommendations for the current sites technologies** |
|---|
| • *Establish an offsite backup system to ensure all critical data is being backed up effectively*<br>• *Implement replication of critical services through a virtual environment*<br>• *Implement electronic archiving to allow archiving of critical documents*<br>• *Implement automated fire suppression systems*<br>• *Implement environmental monitoring*<br>• *Document system recovery procedures for current systems*<br>• *Implement a single integrated directory services environment* |

- *Sign service level agreements with technology suppliers*
- *Implement change control and root cause analysis*

**Strategy recommendations for the recovery site technologies**

- Allow remote connectivity into the environment for remote employees not allocated to the building (Typically plan for 3G, Internet, wireless, VPN services)
- Have adequate networks to support the recovery of the systems required to continue business operations
- Have sufficient facilities to support the hosting of key business systems and associated dependencies
- Permanent area to host offsite storage, backups and servers for replication from ELM

## 12. CONFIDENTIALITY AND NON-DISCLOSURE

This document is confidential and must be treated as such. Distribution and usage of this document is subject to the signed confidentiality clause stipulated in employee contracts.

## 13. ADMINISTRATION OF BUSINESS IMPACT ANALYSIS

The ICT Manager is responsible for maintaining the ICT DR Business Impact Analysis document. The document must be reviewed and approved on an annual basis.

## 14. DELEGATION OF RESPONSIBILITY

In accordance with the ICT Governance Policy, it is the responsibility of the Municipal Manager to determine the delegation of authority, responsibilities and accountability to the Management with regards to the Corporate Governance of ICT.

## 15. EXCEPTIONS

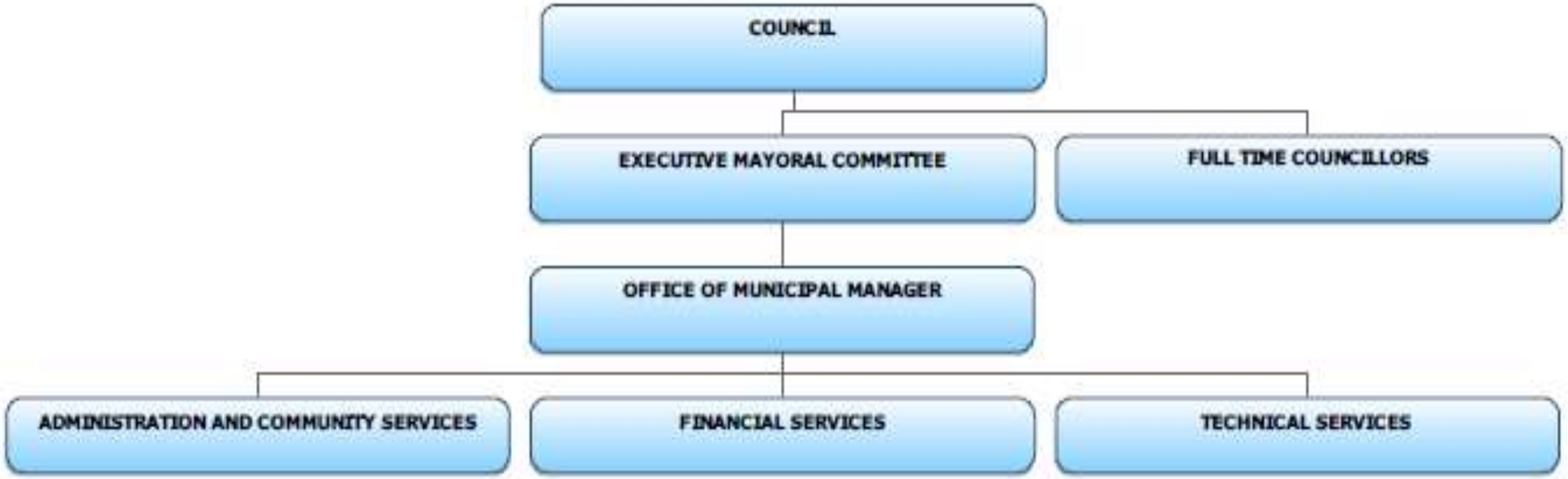
15.1 This Business Impact Analysis does not include the Business Continuity Plan.

## 16. IMPLEMENTATION ROADMAP

| Time Period | Year 1 | | | | Year 2 | | | | Year 3 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Actions | Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Q4 |
| Prep & housekeeping | | | | | | | | | | | | |
| Kickoff with Line Managers , Application Owners & ICT Manager. | ■ | | | | ■ | | | | ■ | | | |
| Assessment Preparation: populate Appendices A.1,A.2,A.3,A.4. | ■ | | | | ■ | | | | ■ | | | |
| Awareness campaign: Key stakeholders & Municipal Mgt | | ■ | | | ■ | ■ | Council resol | | ■ | ■ | .9/05/29/9.12 | |
| Perform Assessment & deliver to ICT & ICT DR Team | | ■ | ■ | | ■ | ■ | | | ■ | ■ | | |

# Appendix A Appendix A: Business Overview

## Appendix A.1 Organogram



COUNCIL
EXECUTIVE MAYORAL COMMITTEE
FULL TIME COUNCILLORS
OFFICE OF MUNICIPAL MANAGER
ADMINISTRATION AND COMMUNITY SERVICES
FINANCIAL SERVICES
TECHNICAL SERVICES

## Appendix A.2 : Buildings and Municipal Operations Locations

| Municipal Function | Main Building Address | Floor or Room Nos | Other Building Address(es) | Flors/Rooms/Outbuildings |
|---|---|---|---|---|
| Administration | 58 Long Street, Moorreesburg, 7310 | Ground | | 2 |
| Community Development, Strategic Services and Technical Services | 64 Long Street, Moorreesburg, 7310 | Ground | | 2 |

## Appendix A.3 Municipal High Level Functions

| Department | Division | Functions |
|---|---|---|
| Administration and Community Services | *Administration* | - *Generate and Distribute of Electronic Agendas*<br>- *Compilation of Annual Report and Oversight Report*<br>- *Secretariat*<br>- *Councillor Support* |
| | *Administration* | - *Records and Archive*<br>- *Switchboard and Reception*<br>- *Reprography*<br>- *Caretaking and Cleaning services* |
| | *Fire Services* | - *Fire Safety and Fire prevention Strategic Planning*<br>- *Enforcement of Fire Protection Regulations*<br>- *Risk Reduction strategies*<br>- *Public Fire Education*<br>- *Scholar Education*<br>- *Industry, Agricultural and Commerce Emergency Readiness Training*<br>- *Community Based Fire Awareness Training*<br>- *Vulnerability and Risk Assessment Audits*<br>- *Cooperation Agreements*<br>- *Review Fire Safety by-laws* |
| | *Air Quality* | - *Ambient Air quality monitoring*<br>- *Emission Reduction / Control Strategies in Domestic fuel, transportation emissions, emissions from mining activities, emissions from agricultural activities, emissions from Industrial activities, waste disposal activities and emissions from biomass burning.* |
| | *Disaster Management* | - *Risk Assessment*<br>- *Risk Reductions (Aligning frameworks and planning)*<br>- *Response and recovery*<br>- *Integration and Comprehensive Information Management and Communication*<br>- *Education, training, public awareness and research* |

| Department | Division | Functions |
|---|---|---|
| | *Municipal Environmental Health* | - *Monitoring of water reticulation systems*<br>- *Monitoring of quality and availability of water intended for human consumption, recreation or industrial use*<br>- *Regulartaking and analysis of water samples*<br>- *Identify and control sources of water pollution*<br>- *Protection of water sources and resources by enforcement of laws an regulations relating to water quality*<br>- *Ensure water supply that is save for human consumption and complies with the Water Services Act, 1997 (Act no. 108 of 1997) and SANS Code 241*<br>- *Implementation of health and hygiene awareness actions and eductaion relating to water quality, water supply and sanitation*<br>- *Food Control*<br>- *Waste Management*<br>- *Health Survaillance of premises*<br>- *Surveillance and Prevention of contagious diseases, excluding immunisation*<br>- *Vector Control*<br>- *Environmental Pollution Control*<br>- *Save handeling of chemical substances*<br>- *Disposal of the dead* |
| | *Ganzekraal Holiday Resort* | - *Administration of Resort*<br>- *Repairs and Maintenance on Resort* |
| Office of the Municipal Manager | *Human Resources* | - *?* |
| | *Internal Audit* | - *Internal Audit provides the municipality with reasonable assurance regarding Risk Management, Controls and Governance.*<br>- *Risk based Audits* |
| | *Community and Social Services* | - *Promoting the Social wellbeing in the community*<br>- *Social Development and community outreach focusing on vulnerable people in the society*<br>- *Early Childhood Development*<br>- *First Aid Training*<br>- *Elderly support (Golden Games)*<br>- *Promote gender equity and to end gender based violence* |

| Department | Division | Functions |
|---|---|---|
| | *Tourism* | - *Pursuing economic growth and facilitation of job opportunities* |
| | *Public Relations* | - *Quarterly newsletter*<br>- *Internal newsletter*<br>- *Campaigns and awareness*<br>- *Digital Communication (Social Media and Website)* |
| | *Expenditure* | - *Manage payments* |
| Finance | *Revenue* | - *Manage cashiering*<br>- *Manage monthly billing*<br>- *Manage customer care* |
| | *Credit control* | - *Manage disconnections*<br>- *Manage indigent consumers*<br>- *Manage legal process* |
| | *Information Technology* | - *Ensure all servers are operational*<br>- *Ensure all Municipal systems are functioning correctly*<br>- *Ensure connectivity is functioning optimally*<br>- *Support of all Municipality users and councillors*<br>- *Ensure security of Municipal systems and information*<br>- *Ensure effective backups of data and critical systems*<br>- *Investigate new technologies and best practices*<br>- *Manage and develop ICT policies*<br>- *Management of ICT assets and infrastructure* |
| | *Pay office* | - *Manage the pay office* |
| | *Supply chain* | - *Procure goods and services*<br>- *Manage the bid office* |
| | *Internal control* | - *Manage internal control* |
| | *AFS* | - *Prepare annual financial statements* |
| | *Budget office* | - *Manage and oversee the budget office* |
| | | - |

## Appendix A.4 Business Applications

This table must represent all high and medium priority business applications used within the Municipality.

| Business application | Application description | Used by |
|---|---|---|
| *Email* | *Electronic messaging system* | *All* |
| *MS Office* | *Office productivity suite* | *All* |
| *SAMRAS* | *Municipal financial management system* | • *Office of the Municipal Manager*<br>• *Administration and Community Development – Administration*<br>• *Human Resources*<br>• *Finance – All*<br>• *Community Services*<br>• *Technical Services* |
| *Collaborator* | *Document tracking system used to track document locations* | • *Administration and Community Development – Records Management*<br>• *Extended Management* |
| *Deedsweb* | *Land and property valuation* | • *Finance* |
| *Fortigate Firewall* | *Fortigate* | • *Finance – Information Technology* |
| *MimeCast* | *Mail filtering* | • *Finance - Information Technology* |
| *Internet* | *Internet access* | *All* |
| *GIS* | *Geographical Information System* | • *Technical Services* |

# Appendix B ASSESSMENT TEMPLATES

## Appendix B.1 Critical Business Functions Requirements

The following table reflect the Municipality's critical business function requirements. This table should also be submitted to the Appendix section of the ICT DR Plan document.

| Critical business functions | Performed by | Frequency | Systems used | MTO | RPO | Onsite users |
|---|---|---|---|---|---|---|
| Support to council and staff | *Administration and Community Services* | *Daily* | *Email* | *1 week* | *None* | *8* |
| Compilation and management of agendas, minutes, items and correspondence | *Administration and Community Services* | *Daily* | *MS Office*<br>*Email* | *1 day* | *None* | *4* |
| Compile and maintain resolution register | *Administration and Community Services* | *Daily* | *MS Office* | *1 week* | *None* | *1* |
| Manage office cleaners | *Administration and Community Services* | *Daily* | *Manual process* | *1 month* | *None* | *1* |
| Manage switchboard | *Administration and Community Services* | *Daily* | *Manual process* | *1 day* | *None* | *2* |
| Manage registry | *Administration and Community Services* | *Daily* | *Manual process* | *1 day* | *None* | *4* |
| Manage filing | *Administration and Community Services* | *Daily* | *Collaborator* | *1 day* | *None* | *2* |
| Manage file storage | *Administration and Community Services* | *Daily* | *Manual process* | *1 day* | *None* | *2* |
| Manage and maintain immovable asset register | *Financial Services* | *Annually* | *SAMRAS* | *1 week* | *None* | *2* |
| Manage recruitment and selection | *Human Resources* | *Weekly* | *Manual process* | *1 week* | *None* | *2* |
| Manage labour relations | *Human Resources* | *Ad-hoc* | *Manual process* | *1 week* | *None* | *2* |
| HR administration | *Human Resources* | *Daily* | *CAPMAN / SAMRAS* | *1 week* | *None* | *2* |

| Critical business functions | Performed by | Frequency | Systems used | MTO | RPO | Onsite users |
|---|---|---|---|---|---|---|
| Manage employee assistance program (EAP) | HR? | Ad-hoc | Manual process | 1 week | None | 2 |
| Records management | Administration and Community Services – Administration | Daily | Collaborator | 1 week | None | 1 |
| Manage training | Human Resources | Weekly | CAPMAN | 1 week | None | 2 |
| Ensure all servers are operational | Finance – Information Technology | Daily | Manual process | 1 day | None | 5 |
| Ensure all Municipal systems are functioning correctly | Finance – Information Technology | Daily | Manual Process to check network systems | 1 day | N/A | 4 |
| Ensure connectivity is functioning optimally | Finance – Information Technology | Daily | Manual Process to check network systems | 1 day | N/A | 4 |
| Ensure security of Municipal systems and information | Finance – Information Technology | Daily | Eset Endpoint<br>Fortigate Firewall<br>MimeCast | 1 day | 24 | 2 |
| Ensure effective backups of data and critical systems | Finance – Information Technology | Daily | Linux scripts<br>F backup | 1 day | 24 | 3 |
| Investigate new technologies and best practices | Finance – Information Technology | Daily | Internet | 1 week | N/A | 2 |
| Manage and develop ICT policies | Finance – Information Technology | Annually | Internet | 1 year | N/A | 2 |
| Management of ICT assets and infrastructure | Finance – Information Technology | Daily | Manual process | 1 month | 744 | 1 |
| Ensure safety and standards | Human Resources | Daily | Manual process | None | None | 1 |
| Ensure compliance to procedures | Office of the Municipal Manager | Daily | EUNOMIA | 1 month | None | 1 |
| Manage performance | Office of the Municipal Manager – Performance Management | Daily | IGNITE | None | None | 2 |
| Monitoring and evaluation | Office of the Municipal Manager – | Daily | MS Office | None | None | 4 |

| Critical business functions | Performed by | Frequency | Systems used | MTO | RPO | Onsite users |
|---|---|---|---|---|---|---|
| | *Performance Management* | | | | | |
| Manage mobilisation for events | *??* | *Ad-hoc* | *Manual process* | *1 week* | *None* | *16* |
| Communicate with communities | *Office of the Municipal Manager* | *?* | *MS Office* | *1 week* | *None* | *16* |
| Liaise with media | *Office of the Municipal Manager – Communications* | *Daily* | *MS Office* | *1 day* | *None* | *4* |
| Communicate with communities | *Office of the Municipal Manager – Communications* | *Daily* | *MS Office* | *1 day* | *None* | *4* |
| Administration of Municipal website | *Finance – Information Technology* | *Daily* | *Website interface* | *1 day* | *None* | *2* |
| Manage publications for the Municipality | *Finance – Information Technology* | *Weekly* | *Website interface* | *1 month* | *None* | *1* |
| Manage cashiering | *Finance - Revenue* | *Daily* | *SAMRAS* | *None* | *None* | *8* |
| Manage monthly billing | *Finance - Revenue* | *Daily* | *SAMRAS*<br>*MS Office*<br>*Email*<br>*Internet* | *5 day* | *None* | *8* |
| Manage customer care | *Finance - Revenue* | *Daily* | *SAMRAS* | *2 days* | *None* | *1* |
| Manage disconnections ? | *Finance - Revenue* | *Daily* | *SAMRAS* | *5 days* | *None* | *5* |
| Manage indigent consumers | *Finance - Revenue* | *Daily* | *SAMRAS* | *10 days* | *None* | *1* |
| Manage legal process | *Finance - Revenue* | *Daily* | *SAMRAS* | *15 days* | *None* | *10* |
| Manage payments | *Finance - Expenditure* | *Daily* | *SAMRAS* | *5 days* | *None* | *6* |
| Manage the pay office | *Finance – Pay Office* | *Daily* | *SAMRAS* | *1 day* | *None* | *6* |
| Procure goods and services | *Finance – Supply Chain* | *Daily* | *SAMRAS* | *3 days* | *None* | *10* |
| Manage the bid office | *Finance – Supply Chain* | *Daily* | *Manual process* | *3 days* | *None* | *4* |

ICT DR Business Impact Analysis

| Critical business functions | Performed by | Frequency | Systems used | MTO | RPO | Onsite users |
|---|---|---|---|---|---|---|
| Manage internal control | *Internal Audit* | *Daily* | *SAMRAS* | *5 days* | *None* | *3* |
| Prepare annual financial statements | *Finance – AFS* | *Daily* | *SAMRAS* | *5 days* | *None* | *5* |
| Manage and oversee budget office | *Finance – Budget Office* | *Daily* | *SAMRAS* | *3 days* | *None* | *3* |
| Meetings with Executive Management | *Office of the Municipal Manager* | *Daily* | *MS Office*<br>*Emails* | *1 month* | *None* | *5* |
| Implement action plans ? | *Development, Strategic Services* | *Daily* | *MS Office*<br>*Emails* | *5 days* | *None* | *9* |
| Communicate with stakeholders | *Office of the MM* | *Daily* | *MS Office*<br>*Emails* | *5 days* | *None* | *5* |
| Submit applications ? | *Strategic Services* | *Daily* | *MS Office*<br>*Emails* | *5 days* | *None* | *5* |
| Compile IDP | *Strategic Services* | *Daily* | *MS Office*<br>*Emails*<br>*GIS* | *1 week* | *None* | *4* |
| Public participation | *Office of the Municipal Manager* | *Bi-annually* | *MS Office*<br>*Emails* | *6 months* | *None* | *3* |
| Deal with general public | *Office of the MM - Communication* | *Daily* | *MS Office*<br>*Emails*<br>*GIS* | *1 day* | *None* | *4* |
| Compile SDBIP | *Office of the MM – Strategic Services* | *Quarterly* | *MS Office*<br>*Emails* | *1 week* | *None* | *2* |
| | | | | | | |
| Fire management | *Administration and Community Development – Fire Services* | *Daily* | *Hazdata system* | *None* | *None* | *24* |
| Disaster management | *Administration and Community Development – Disaster management* | *Daily* | *Manual process* | *None* | *None* | *24* |

## Appendix B.2 ICT service recovery requirements

| Service | Description | Used by | Recovery dependencies | Recovery time requirements | | |
|---|---|---|---|---|---|---|
| | | | | MTO (hrs) | RTO (hrs) | RPO (hrs) |
| *LAN/WAN* | *Network to cater for connectivity to all systems* | *All employees* | *Routers, switches, diginet link, firewall, Telkom NTU* | *24* | *16* | *N/A* |
| *Desktops* | *Desktops to provide client functionality for users* | *All employees* | *Operation systems, client software, network connectivity, servers* | *24* | *16* | *None* |
| *Mail server* | *Electronic messaging system* | *All employees* | *Mail server software, operating system, databases, storage, network connectivity, antivirus* | *24* | *16* | *None* |
| *MS Office* | *Office productivity suite* | • *All* | *Operating system, storage, network connectivity, antivirus* | *None* | *None* | *None* |
| *Opticon* | *Switchboard management system* | • *Administration and Community Development - Administration* | *Databases, storage, network connectivity,* | *24* | *16* | *None* |
| *SAMRAS* | *Municipal financial management system* | • *Administration and Community Development – Administration, Municipal Health, Fire Services, Disaster Management*<br>• *Office of the Municipal Manager – Human Resources*<br>• *Finance – All* | *SAMRAS software, operating system, databases, storage, network connectivity, antivirus* | *24* | *16* | *None* |

| Service | Description | Used by | Recovery dependencies | Recovery time requirements | | |
|---|---|---|---|---|---|---|
| | | | | MTO (hrs) | RTO (hrs) | RPO (hrs) |
| | | • Technical Services<br>• Office of the Municipal Manager - All | | | | |
| *Fortigate* | *Physical Firewall device* | • *Financial Services – Information Technology* | *Fortigate Firmware, network connectivity,* | *24* | *16* | *24* |
| *MimeCast* | *Mail filtering and Antivirus* | • *Finance – Information Technology* | *Internet* | *24* | *16* | *24* |
| *Internet* | *Internet access* | • *All* | *Operating system, network connectivity, antivirus* | *24* | *16* | *N/A* |
| *BulkSMS* | *Bulk SMS messaging system* | • *Finance – Credit Control* | *Internet Access, Email* | *120* | *112* | *None* |
| *GIS* | *Geographical Information System* | • *Development, Planning and Housing – Town Planning* | *GIS software, operating system, databases, storage, network connectivity, antivirus* | *24* | *16* | *None* |

## Appendix B.3 Applications Required per Department

**Legend:**

| | |
|---|---|
| Required | ✓ |
| Not required | ✗ |

| Division | ERP | Collaborator | CAPMAN | IGNITE | EUNOMIA |
|---|---|---|---|---|---|
| Office of the MM | ✓ | ✓ | ✗ | ✓ | ✓ |
| Administration | ✗ | ✓ | ✗ | ✓ | ✓ |
| Technical Services | ✗ | ✓ | ✗ | ✓ | ✗ |
| Human Resources | ✗ | ✓ | ✓ | ✓ | ✗ |
| Financial Services | ✓ | ✓ | ✗ | ✓ | ✓ |

**Table 2: Application requirements for Departments**