Information Communication and Technology (ICT)

Matjhabeng Local Municipality

(MLM)

IT Disaster Recovery (DR) Strategy

Document Version: 0.5 (Draft)

Table of Contents

Document Information

Project Name:	ICT DR and BCP Matjhabeng		
Prepared By:	Matjhabeng ICT	**Document Version No:**	0.5
Title:	DR and BCP for Matjhabeng ICT	**Document Version Date:**	01/08/2018
Reviewed By:		**Review Date:**	

Distribution List

Name	Date	Phone/Fax/Email

Document Version History

Version Number	Version Date	Revised By	Description	Filename
0.1	11/04/2018	Matjhabeng ICT	Document creation	DR and BCP for Matjhabeng
0.2	27/04/2018	Matjhabeng ICT		
0.3	12/05/2018	Matjhabeng ICT		
0.4	07/06/2018	Matjhabeng ICT		
0.5	01/08/2018	Matjhabeng ICT		

1. INTRODUCTION

The Matjhabeng IT Department's primary function is to ensure reliable and consistent delivery and support of Information Communication & Technology (ICT) services and/or infrastructure throughout the Municipality, thereby enabling the municipality to optimally execute its mandate. The IT Department therefore continually provides and deploys ICT enabling tools to manage and improve business processes.

As part of becoming more competitive and better supporting the municipality and business priorities, The IT Department has initiated the development of a Disaster Recovery Management Program., thus ensuring business continuity by implementing a Disaster Recovery Plan for mission critical systems.

This DR Strategy and Plan will make provision for resilience against events that could disrupt business as usual activities. The resilience and response approach is to be proportionate to the risk and to a level agreed by the municipality.

2. OBJECTIVES

The objective of this DR Strategy and Plan is to ensure that the risks identified in the Business Impact Analysis (BIA) are mitigated. The analysis focused on critical applications within the municipality. Based on the analysis conducted, the following objectives are targeted:

- Develop capability within the local environment to meet business RTOs and RPOs
- Establish a Disaster Recovery capability at an offsite location for the Head Office server farm.

The diagram below shows a high-level view of the BCM methodology:

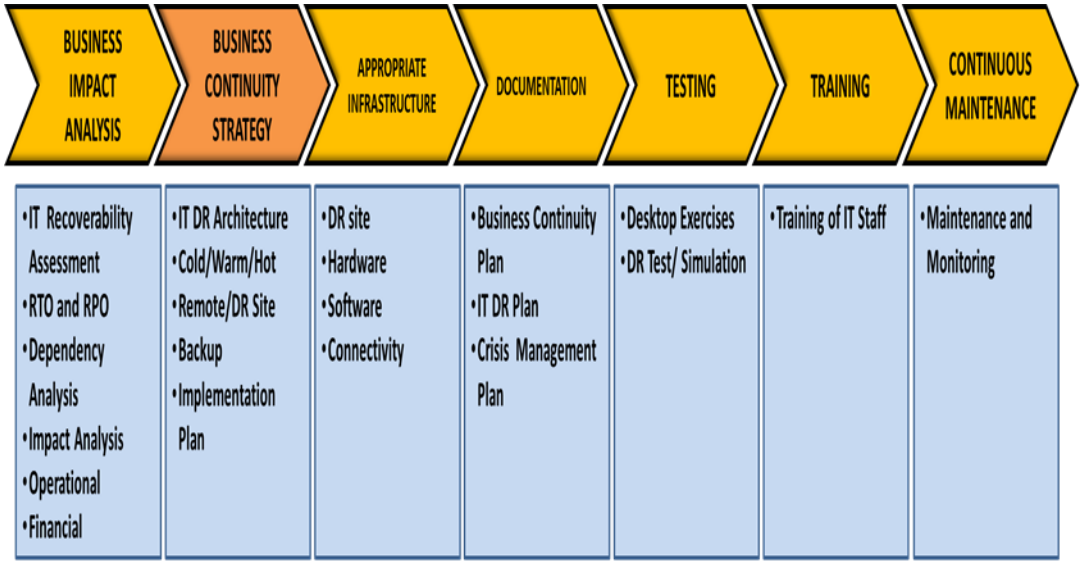

Figure 1: Methodology

3. HIGH LEVEL VIEW OF THE CURRENT STATUS

The municipality has all critical applications and infrastructure hosted at the Head Office Data Centre, 319 Stateway, Welkom. There is a secondary DR site that has been identified in Virginia, 6 Union Street (Main Building), Virginia - however the DR site is not equipped with infrastructure and not yet ready to host any equipment.

The existing environment at the Head Office is not designed to provide a high level of availability - the environment is not adequately resourced to continue normal operations should there be a complete loss of the primary data centre.

The potential data loss could extend to an entire day, and recovery of the entire IT environment at an offsite location from archived backup is untested.

Addressing these shortfalls will contribute towards the achievement of the defined objectives.

The following specific single points of failure have been identified within the current IT environment and must be addressed to achieve the recommended level of resilience:

- Insufficient switch redundancy for servers.
- There are currently no backup servers or clusters in the event of component failures.
- The RTOs and RPOs currently not achieved for critical applications listed in the table below:

RTO	RPO
Solar/ Cash Drawer	Solar/ Cash Drawer
Syntell	Syntell
PayDay	PayDay
MS Office 365	File Sharing/ Local Drives
File Sharing/ Local Drives	
Paperless Agenda	

Table 1: List of applications

4. LEVELS OF RESILIENCE

The level of resilience desired by the municipality will determine the most suitable strategy to be adopted in order to achieve the defined objectives, with the higher the level resulting in an increased ability to meet offsite RTOs and RPOs.

The following levels of resilience are defined, ranked from the lowest level of resilience to the highest:

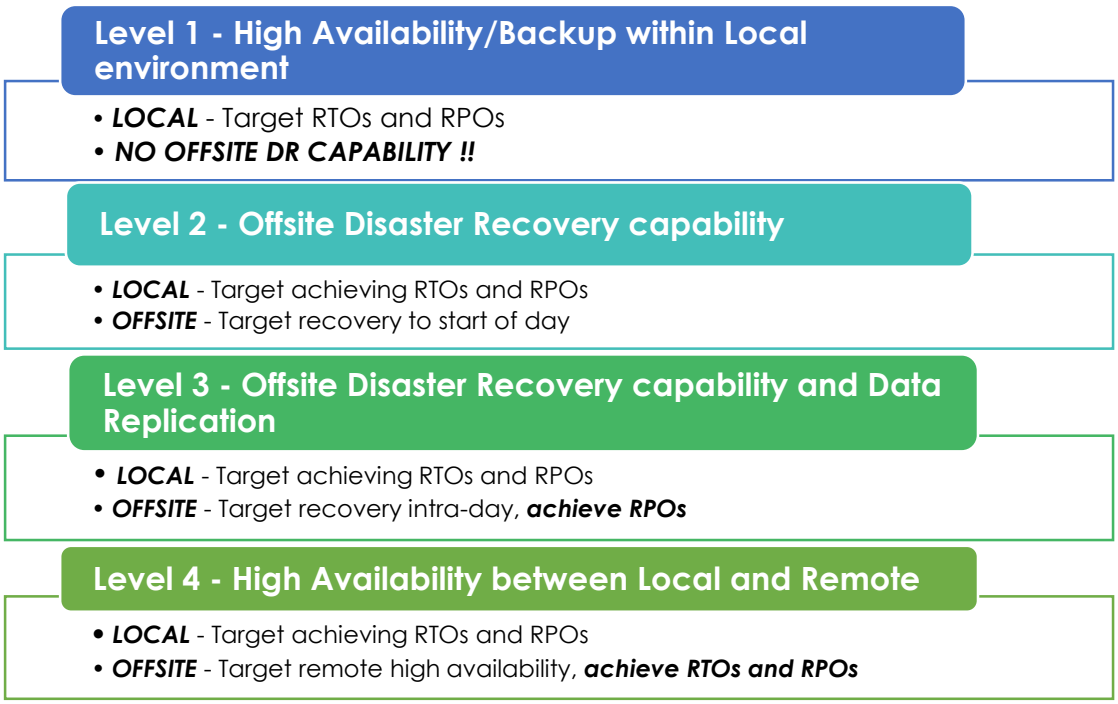

Figure 3: Levels of Resilience

Level 1 is based on shared backup infrastructure and cluster level fail-over in the production environment; no offsite DR capability.

Levels 2-4 include addressing the identified shortfalls within the current environment and level 1 with regards to offsite capability and meeting the required RTO and RPOs.

4.1 RESILIENCE LEVEL RATING

The following table illustrates the rating of the various levels of resilience:

Key	
☺	**Good**
😐	**Average**
☹	**Bad**

	Level 1	*Level 2*	*Level 3*	*Level 4*
Potential data recoverability	☹	😐	😐	☺
Cost	☺	😐	😐	☹
Implementation Time	☺	☺	😐	☹

Table 4: Resilience Level Rating

4.2 TARGET RECOVERY TIMES AND DATA LOSS

The following target recovery times and data loss estimates are associated with each level of resilience at an offsite location:

Level	*Target Recovery Time*	*Potential Data Loss*
Current	Unknown	Unknown
Level 1	Unknown	Unknown
Level 2	48 hours	1 Day
Level 3	Meet RTOs	1 Day
Level 4	Meet RTOs	Meet RPOs

Table 5: Target Recovery

5. RESILIENCE OVERVIEW

Various strategies are proposed in order to attain the desired level of resilience. These levels are not mutually exclusive, and different strategies may be applied to different systems and applications depending on the defined business requirements.

Each level presented comprises the following infrastructural elements:

- Systems – IT server equipment and software
- Storage – Disk hardware and software
- LAN and WAN – Switches, routers
- Telecoms – Remote data centre connectivity
- Data Centre – Computer room space, power and cooling
- Professional Services – Project management, specialist skills

The approach ultimately selected by the municipality is directly dependent on the desired level of resilience.

5.1 LEVEL 1 – HIGH AVAILABILITY/ WARM BACKUP WITHIN EXISTING ENVIRONMENT

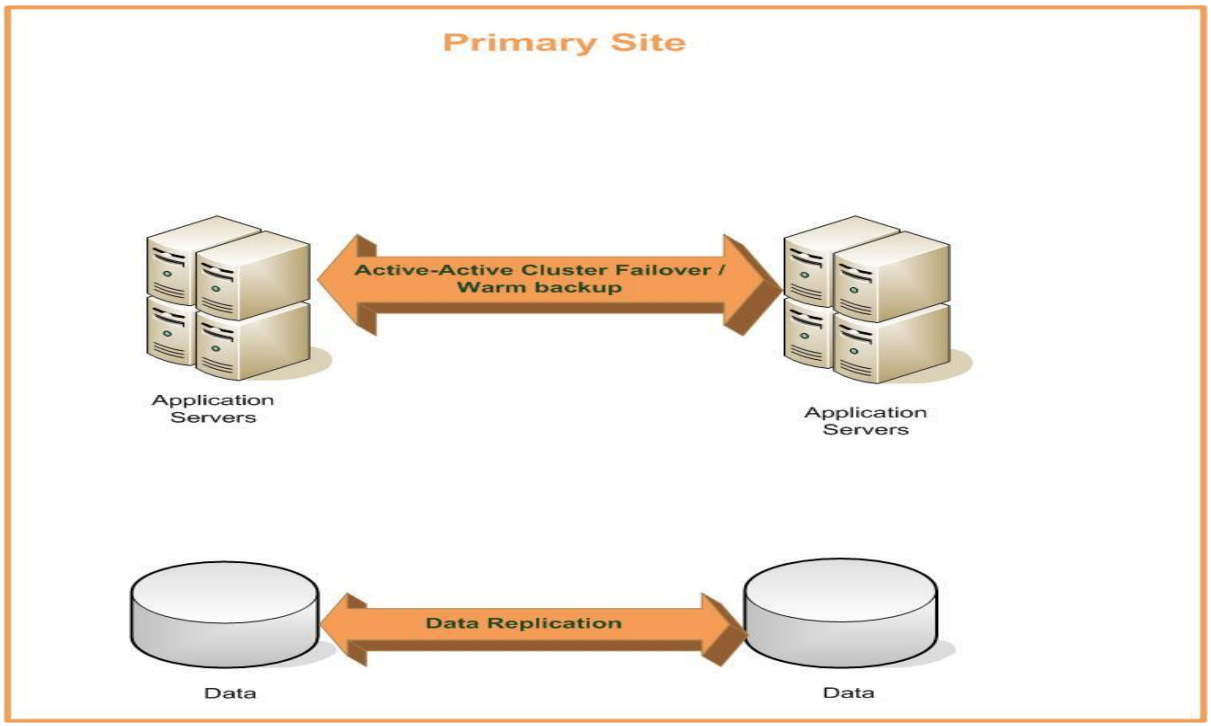

Figure 4: Level 1 Resilience

5.1.1 Overview

This level of resilience is designed to provide a high level of availability, owing to a combination of redundant IT hardware, data replication and software clustering.

This level will not be adequately resourced to continue normal operations following a complete loss of a data centre.

5.1.2 RTO and RPO Targets

Improving the resilience within the existing environment will ensure that business defined RTOs and RPOs can be achieved in the event of component failures, including the applications which are currently at risk mentioned in section 3.

5.1.3 Features

- Fast recovery from an incident affecting a single data centre.
- Improved confidence in ability to fail-over as much of the resilience equipment is being actively used.

- Recovery procedures can be simplified and/or automated, as much of the infrastructure will be up and running.
- Less overhead on change and configuration management as the infrastructure is being continually exercised and so issues are likely to be identified more quickly than where equipment is not be used.
- Live fail-over rehearsals are easier to implement.

5.1.4 Disadvantages

- Insufficient provision is made against total loss of the data centre.
- Data corruption and software bugs can affect both environments.
- Can be more difficult to implement and manage than other models.
- May require additional load balancing technology to split services.
- Complex database and application issues may arise.
- Finding the same hardware to restore to at an alternate site would be mostly impossible as the vendors change models regularly.

5.2 LEVEL 2 – OFFSITE DISASTER RECOVERY CAPABILITY

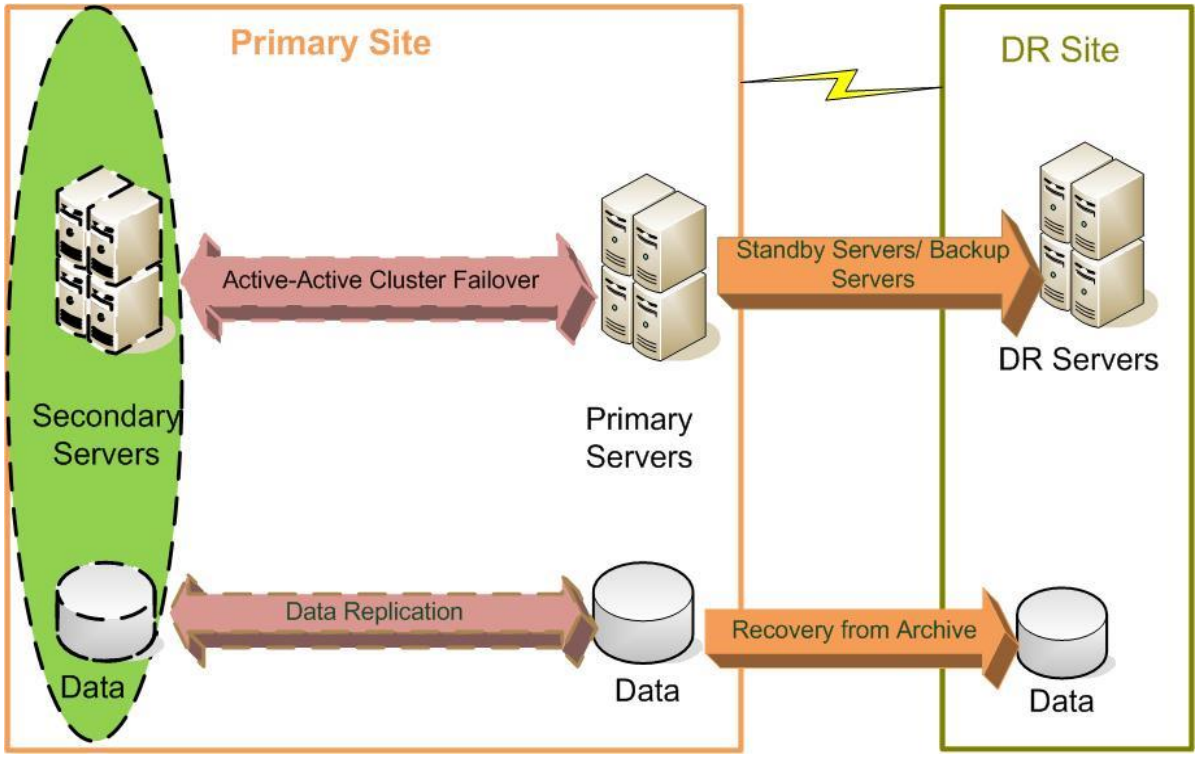

Figure 5: Level 2 Resilience

5.2.1 Overview

This level of resilience provides for an offsite DR capability in order to cater for a worst-case scenario that disables the production data centre. The recovery of systems will be from archived backups to a specific point in time.

Additional IT equipment and infrastructure will be required and could be shared in order to provide a more cost-effective recovery environment. A highly efficient level of change control and regular testing will be required in a syndicated environment.

5.2.2 Approach

This level provides for SAN at an offsite recovery location used for the recovery of data from archived backup.

Dedicated servers are maintained in either a cold or warm state at the remote recovery site, ready for operation in a short space of time.

A high-speed WAN link is recommended for system updates and online backup to the remote recovery centre.

5.2.3 RTO and RPO Targets

Business defined RTOs and RPOs cannot be achieved in the event of a complete failure at the production data centre, however recovery from archived backup will be possible subject to longer recovery timeframes and greater potential data loss.

The potential loss of data could extend to an entire day, as the strategy for this level is based on recovery from the previous night's archived backup.

5.2.4 Features

- Provision is made for a major incident that disables the production data centre.
- Provision of an isolated recovery and test environment.
- Ability to test system recovery to a point in time from archived backup.
- Short timeframe to implement physical environment.

5.2.5 Disadvantages

- Slowest recovery from an incident.
- Lengthy timeframe associated with recovery from backup archive.
- Server and network environment will still need to be manually recovered.
- Change and configuration will require time and resources.
- Maturity in achieving successful recoveries will require regular rehearsals.

5.3 LEVEL 3 – OFFSITE DR CAPABILITY AND DATA REPLICATION

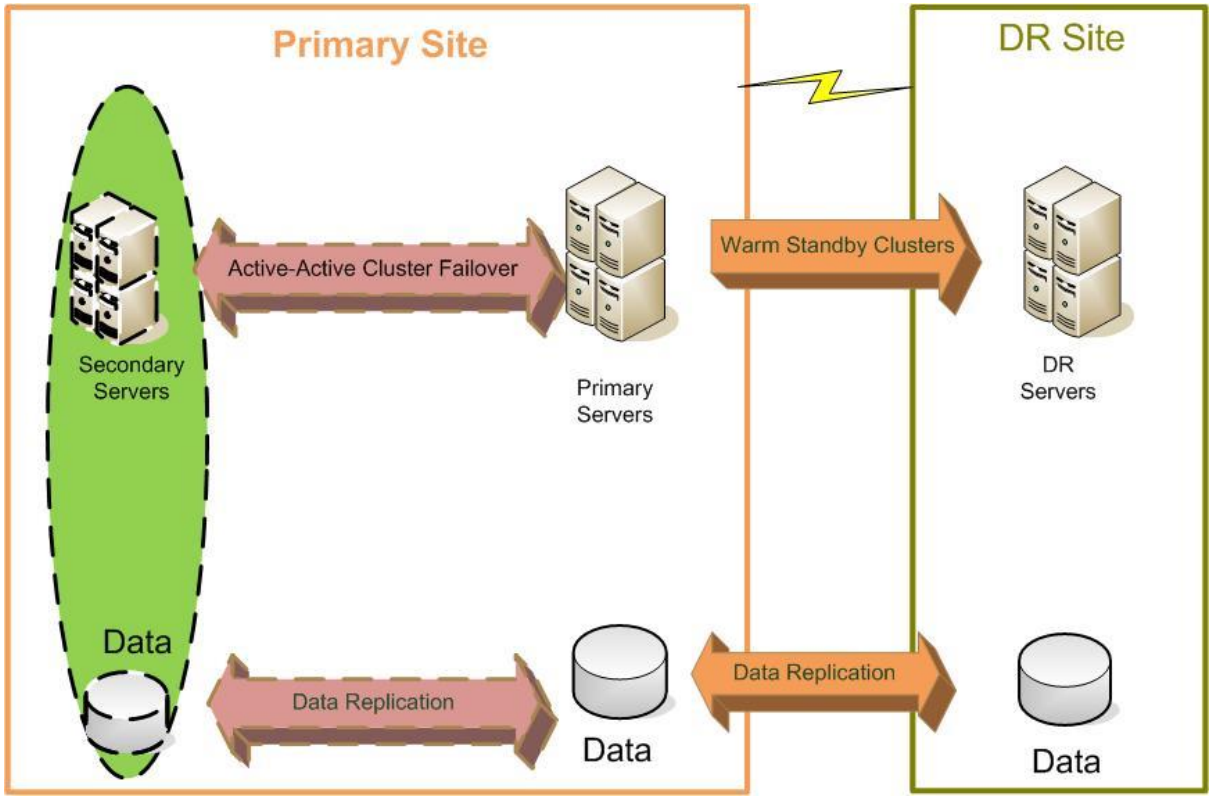

Figure 6: Level 3 Resilience

5.3.1 Overview

This level of resilience provides the municipality with an offsite storage of replicated data (some synchronously) in order to reduce the recovery time in the event of a major incident affecting the production data centre.

Replication of data will require investment in disk storage, replication software and significant bandwidth between the two sites.

5.3.2 Approach

This level provides for high specification SAN at an offsite recovery location used for the replication of data from the production environment.

Dedicated servers are maintained in a warm state at the remote recovery site, ready for operation in a short space of time.

A high-speed WAN link is recommended in order to facilitate data replication and DR system updates.

5.3.3 RTO and RPO Targets

Recovery from replicated disk storage will be possible and RPOs can be achieved.

The potential loss of data may extend to the start of day, as the strategy for this level is based on a worst-case scenario of recovering to a consistent state from the replicated data store.

5.3.4 Features

- All the advantages associated with the high availability environment are retained.
- Provision is made for a major incident that disables the production data centre.
- A copy of data is stored off-site.
- Provision of an isolated recovery and test environment.
- Ability to test recovery to point in time at the remote site.

5.3.5 Disadvantages

- Additional costs associated with a remote site.
- Some manual intervention to facilitate recovery is still required (not seamless).

5.4 LEVEL 4 – HIGH AVAILABILITY BETWEEN LOCAL AND REMOTE SITES

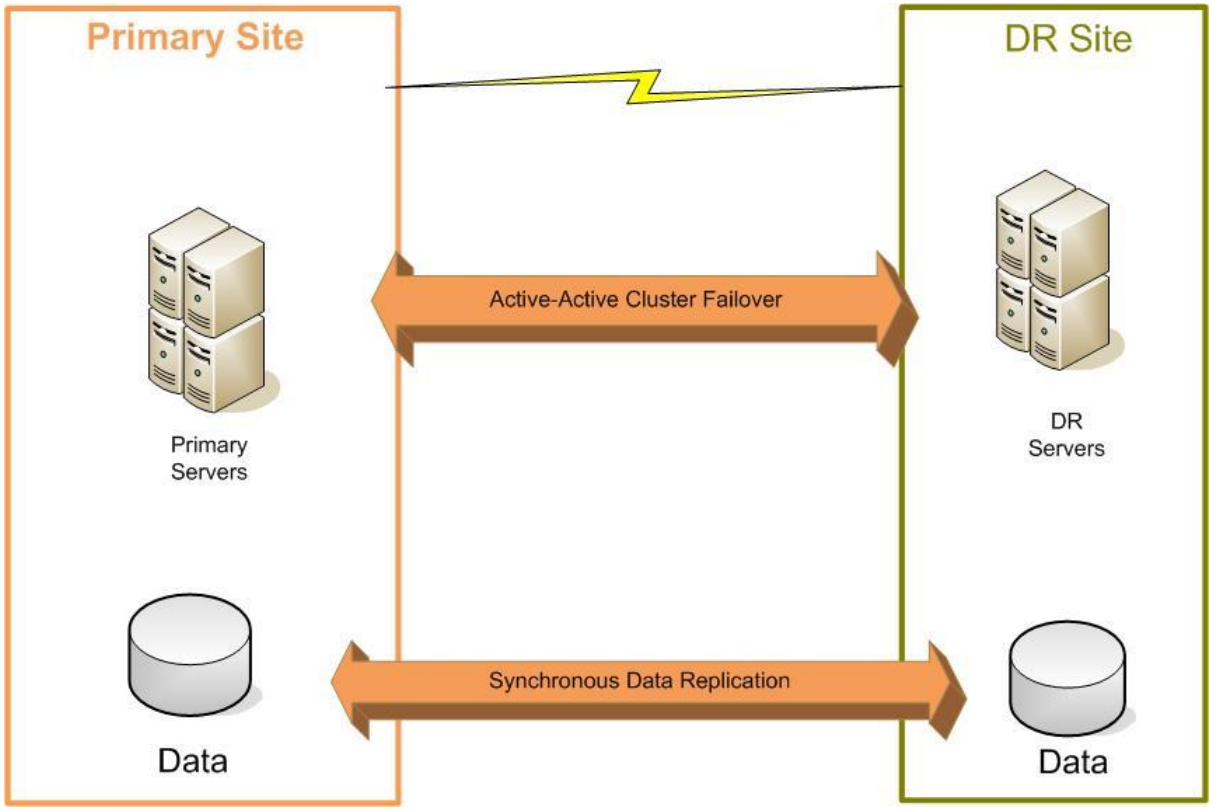

Figure 7: Level 4 resilience

5.4.1 Overview

This level of resilience provides for a remote high availability environment which is situated at a suitable distance from the production data centre.

Consolidation of HA capabilities at the production site could facilitate the transfer of some hardware and infrastructure and additional elements will be required to ensure the elimination of any single points of failure. The most significant cost would be the provision of high capacity, resilient bandwidth between the two sites.

5.4.2 Approach

This level provides for high specification SAN at an offsite recovery location used for the synchronous replication of data from the production environment.

Dedicated servers are clustered remotely with systems able to failover should the Production data centre be disabled.

A high-speed resilient network link is required between the production and remote environments to facilitate data replication, server clustering and processing failover.

5.4.3 RTO and RPO Targets

Business defined RTOs and RPOs can be achieved in the event of an outage affecting the production data centre.

The potential for data loss is eliminated as this level of resilience provides for synchronous data replication and cluster failover between the production and offsite DR locations.

5.4.4 Features

- Fast recovery from an incident
- Improved confidence in ability to fail-over as much of the resilience equipment is being actively used at each site.
- Recovery procedures can be simplified and/or automated, as much of the infrastructure will be up and running.
- May improve utilisation of the infrastructure.
- Less overhead on change and configuration management as sites are being continually exercised and so issues are likely to be identified more quickly than where equipment is not be used.
- Live fail-over rehearsals are easier to implement.

5.4.5 Disadvantages

- Significant cost associated with bandwidth connectivity between sites and relocation of installed infrastructure and equipment.
- Can be more difficult to implement and manage than other models.
- May require additional load balancing technology to allow services to be split across remote sites.
- Complex database and application issues may arise.
- Network latency may be an issue.

6. RECOMMENDED STRATEGY IMPLEMENTATION

The proposed strategy targets the achievement of a hybrid level of resilience for the different applications. This was driven by the input from the business units within the municipality and the applications were matched to the appropriate level of resilience depending on the requirements.

It is recommended that the municipality implement the solution in a phased approach, starting with phase 1 as getting the recovery site in Virginia ready can be a long process. The recommended implementation plan below initially focuses on the solutions that can be implemented in a short period of time to achieve RTO and RPO in the local environment, also with the view of achieving DR capability in the long term.

Levels 3 and 4 of resilience represent an idealistic scenario that should form the basis of a long-term strategy and should be actively considered when planning future production IT strategies. The continued improvement in cost of telecom services, as well as advancements in IT technology, software services and server virtualisation will contribute towards achieving this level of resilience.

Additional human resources and management will be required to develop the skills, processes and plans associated with establishing and maintaining a successful IT service continuity strategy.

6.1.1 Phase 1:

Objective	To achieve high availability for applications with RTO and RPO lower than 8 hours.
Actions	• Upgrade the existing servers e.g. dual network cards, dual power supply, RAID 5 • Upgrade the switching in the data centre to provide redundancy. • Upgrade power and air-conditioning to remove single points of failure. • Establish a redundant point of presence (Link) at the DR site. • Configure high availability for the applications listed in (a) below.

(a) Applications recommended for this phase

Based on the analysis, the following applications within the municipality are recommended for this phase:

Application	Current Level	Current Location
Solar/ Cash Drawer	Level 1	HO Data Centre
Syntell	Level 1	HO Data Centre
PayDay	Level 1	HO Data Centre
MS Office 365 (Internet Links)	Level 1	HO Data Centre
File Sharing/ Local Drives	Level 1	HO Data Centre
Paperless Agenda (Internet Links)	Level 1	HO Data Centre

Table 6: Level 1 Applications

6.1.2 Phase 2:

Objective

Based on level 2 as described in section 5.2, obtain/prepare a Disaster Recovery site.

Actions

- Acquire a Disaster Recovery site for the Head office.
- Establish DR capability at the Virginia site.
- Acquire necessary hardware for Level 2 resiliency e.g. tape backup infrastructure, servers for DR site.
- Configure servers hosting the applications listed in (a) below for level 2 of resilience.

(a) Applications recommended for this level

Based on the analysis, the following applications within the municipality are recommended for this level:

Application	Current Level	Current Location
Solar/ Cash Drawer	Level 1	HO Data Centre
Syntell	Level 1	HO Data Centre
PayDay	Level 1	HO Data Centre
MS Office 365 (Internet Links)	Level 1	HO Data Centre
File Sharing/ Local Drives	Level 1	HO Data Centre
Paperless Agenda (Internet Links)	Level 1	HO Data Centre

Table 7: Level 2 Applications

6.1.3 Phase 3:

Objective: Transfer the HA/UAT hardware to the DR site to achieve level 3 as described in section 5.3.

Actions:

- Acquire necessary hardware for replication and backup.
- Upgrade the WAN network infrastructure.
- Acquire necessary hardware for Level 3 resiliency e.g. tape backup infrastructure, servers and SAN the for DR site
- Configure servers hosting the applications listed in (a) below for level 3 of resilience.

(a) Applications recommended for this level

Based on the analysis, the following applications within the municipality are recommended for this level:

Application	Current Level	Current Location

Application	Current Level	Current Location

Table 8: Level 3 Applications

6.1.4 Phase 4:

Objective	Implement high availability between the sites as described in section 5.4.
Actions	• Upgrade the WAN network infrastructure to cater for high availability between sites. • Configure servers hosting the applications listed in (a) below for level 4 of resilience. • Move the servers configured for high availability in level 1 to the DR site.

(a) Applications recommended for this level

Based on the analysis, the following applications within the municipality are recommended for this level:

Application	Current Level	Location

Table 9: Level 4 Applications

6.2 TELECOMMUNICATIONS

6.2.1 Connectivity to Telkom

6.2.2 Connectivity to Remote Sites (Telkom VPN)

6.3 GENERAL RECOMMENDATIONS

- It is recommended that the municipality develop business continuity plans for the different business units – This IT DR Strategy and Plan will be the subset of the overall business continuity plan.
- It is recommended that the municipality perform Disaster Recovery tests annually to validate that the DR hardware implemented meets the business requirements.
- The backup strategy must be revisited, and the municipality must consider offsite storage of the backup tapes.
- Single points of failure must be addressed within the current environment; addressing these shortfalls will contribute towards the achievement of the defined objectives.
- The detailed design of this solution should take virtualisation and data lifecycle management into consideration in order to provide a resilient and manageable environment in which to fail over processing or recover systems to a specific point in time.
- The production server room must be supported by UPSs and generator electricity to maintain systems in a power outage – the room must also be supported by adequate air-cooling systems.
- The municipality must ensure that all servers are hosted in the dedicated data centre and not scattered in the office environments.

6.4 BEST PRACTICE

The following standards and codes of practice are referenced in suggesting a long term strategy:

6.5 *ISO 24762*

"DR sites should be in geographic areas that are unlikely to be affected by the same disaster/failure events as organizations' primary sites. The issue of site proximity and associated risks should be taken into consideration when ICT DR service providers contract and agree SLAs with organizations."

6.6 *The PAS77: 2006 IT Service Continuity Management Code of Practice*

"Location and distance between sites: If failing over from one site to another the network path distance between the two sites should be carefully considered. If the two sites are too close together, for example on a campus, they could be impacted by the same natural disaster. If too far apart then the cost of connecting the two sites with suitable telecommunications and/or courier services could become prohibitive. Most importantly the distance between the sites could have a negative impact on the way in which the IT systems operate. If the chosen model includes synchronous replication, then the greater the distance the greater the latency, thus introducing delays in the transfer of data between sites which could in turn impact application performance."

"Business Continuity Management (BCM) is concerned with managing risks to ensure that at all times an organization can continue operating to, at least, a pre-determined minimum level."

7. APPROVALS

The signatories hereof, being duly authorised thereto, by their signature hereto authorise the implementation and/or adoption of this plan.

Municipal Manager, who hereby approves this DR Strategy	Date
Executive Director: SSS, who hereby recommends and approves this DR Strategy	Date
Acting ICT Manager: who hereby recommends this DR Strategy	Date