Province of the
EASTERN CAPE
COOPERATIVE GOVERNANCE
& TRADITIONAL AFFAIRS

DISASTER RECOVERY PLAN 2025

Departmental Contact Details	
Physical Address	Tyamzashe Building Phalo Avenue Bhisho 5605
Postal Address	Department of Local Government and Traditional Affairs Private Bag X0035 Bhisho 5605
Document Number	CGICT-DRP-002
Document Name	Disaster Recovery Plan
Contact Person	Ms T.M. Luke
Designation	Director: GICTM
Component	Government Information and Communication Technology Management (GICTM)
Telephone No.	040 940 7235
Cell Phone No.	076 141 1749
E-mail Address	tswakai.luke@eccogta.gov.za
Date Completed	
Date of Approval	
Date Last Amended	2021/03/31
Date For Next Review	

SIGN OF

HEAD OF DEPARTMENT

This Disaster Recovery Plan has been recommended by Vuyo Mlokothi in my capacity as the Head of Department of the Eastern Cape Department of Cooperative Governance and Traditional Affairs.

I am satisfied and concur with the contents of this Plan.

The development of the Disaster Recovery Plan will ensure the department is able to exercise its powers in compliance with the law and guide decision- making in the department.

SIGNED	
DESIGNATION	Mr. V. Mlokothi, Head of Department: Cooperative Governance and Traditional Affairs
DATE	10/08/2025

EXECUTIVE AUTHORITY

The Department of Cooperative Governance and Traditional Affairs has an unprecedented opportunity to improve the livelihoods of the people by effectively rendering the many services that it is expected to provide. We have envisaged a department that has the required capacity to respond adequately to the challenges of its people.

I therefore trust that guidance from this Disaster Recovery Plan will contribute to the effective fulfilment of the departmental mandate, the service delivery expectations of the public and the performance expectations within the department.

SIGNED	
DESIGNATION	Member of the Executive Council : Honourable Z.A. Williams of Cooperative Governance and Traditional Affairs
DATE	12. 08. 2025.

Cn

Contents

ANNEX A : ABBREVIATIONS AND DEFINITIONS

TERM	DEFINITION
Abbreviations	
A.D	Active Directory
BCM	Business Continuity Management
BCP	Business Continuity Plan
COGTA	Department of Cooperative Governance and Traditional Affairs
DBA	Database Administrator
DR	Disaster Recovery
DRP	Disaster Recovery Plan
DSC	District Support Centre
EC	Eastern Cape
GICTM	Government Information and Communication Technology Management
GIS	Geographic Information System
HEAD OF ICT	The ICT Director, also referred to as Government Information Technology Officer (GITO)
ISO	International Standard Organisation
IT	Information Technology
ITCP	IT Continuity Plan
LAN	Local Area Network
MISS	Minimum Information Security Standard
PFMA	Public Finance Management Act
PSCBC	Public Service Coordinating Bargaining Council
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SANS	South African Bureau of Standards / South African National Standards
SCM	Supply Chain Management
SITA	State Information Technology Agency
SLA	Service Level Agreement
SQL	Structured Query Language
WAN	Wide Area Network
Definitions	

GIS Server	Specialised server that stores, processes, and serves geospatial data and maps to users and applications over a network
On-Prem	Software and IT infrastructure that is installed and operated within a company's own facilities, rather than relying on third-party cloud services
RPO	Recovery Point Objective: The snap point at which the business unit critical process data is available. This refers to the amount of tolerable data loss by the business unit
RTO	Recovery Time Objective: The time required for the business unit critical process to be up and running
AD Connect	Microsoft tool used to integrate on-premises directories (like Active Directory) with Azure Active Directory (Azure AD)
Storage Media	physical devices used to hold and preserve digital data
SQL Server	Relational database management system (RDBMS) from Microsoft
Virtual Machine	Software emulation of a physical computer. It runs an operating system and applications just like a physical computer but is hosted on a physical machine (called a host) using virtualization software like VMware or Hyper-V
VM Recovery	Process of restoring a virtual machine (VM) to a previous working state after a failure, data loss, corruption, or disaster.

REFERENCES AND RELATED LEGISLATION AND REGULATIONS

The following publications govern the execution of the COGTA Disaster Recovery Plan:

- Constitution of the Republic of South Africa 1996
- SANS/ ISO 22301
- SANS/ISO 27002
- Minimum Information Security Standards
- Minimum Interoperability Standards
- Protection of Information Act
- Public Service Act and Public Service Regulations
- Regulation of Interception of Communications Act
- ISO 38500 IT Governance Standard
- Electronic Communications and Transactions Act
- COGTA Strategic Plan

1 DISASTER RECOVERY PLAN OVERVIEW

The Disaster Recovery Plan is the result of the ongoing process of planning, developing, testing and implementing emergency recovery procedures and processes. This process ensures the efficient and effective resumption of critical systems in the event of a major interruption to the IT infrastructure at the Department of Cooperative Governance and Traditional Affairs. The DRP serves as an action plan to guide the recovery team in restoring the operating systems, applications and data of their critical systems.

The DRP addresses recovery of IT system(s) after disruption and does not focus on business process recovery. It establishes procedures and capabilities for recovering critical IT applications within the COGTA.

The COGTA head office building is situated at the following physical location:
Tyamzashe Building, Phalo Avenue, Civic Square, Bisho, 5605, Eastern Cape
The department has district offices in Port Elizabeth (+/- 19 users), Mthatha (+/- 18 users), Alfred Nzo (+/- 14 users), Chris Hani (+/- 11 users), Amatole (+/- 17 users) and Joe Gqabi (+/- 7 users). In total the department has total number of +/- 1148 IT users.

1.1 ORGANISATION OF THE RECOVERY PLAN

The COGTA business objectives (Eleven Priority Areas) are as outline below:

COGTA Eleven Priority Areas		
	a)	Full implementation of PMDS (Performance Management and Development System)
	b)	Implementation of an integrated HR plan (and roll out of integrated wellness programme)
	c)	Implementation of departmental strategic goals and objectives (Strategy and Systems)
	d)	Implementation of sound corporate governance (Continuous improvement of corporative governance and integrated procurement planning)
	e)	Full implementation of Minimum Information Security Standards (MISS).
	f)	Supporting integrated service delivery through IGR and Communication Services
	g)	Strengthen and improve spatial frameworks, strategies and capacity for LED and Rural Development.
	h)	Improve municipal capacity for infrastructure programmes, indigent strategies and disaster management systems.
	i)	Facilitate the turnaround of the audit outcomes of municipalities.
	j)	Promote transformation and accountability in municipalities
	k)	Facilitate and support the transformation and development of effective Traditional Institutions.

The Disaster Recovery Plan shall address the business objectives as outline above:

The DRP programme should form a comprehensive solution for the Department and at least includes all of the following elements:

- ✓ Critical Information Assets to be protected and Degree of assurance required.
- ✓ Backup and retention of information and software as per MISS and National Archives regulations for electronic data.
- ✓ Recovery procedures and responsibilities to facilitate the rapid restoration of normal operations.
- ✓ Minimally acceptable level of degraded operation of the essential systems or functions must be identified and prioritised to guide implementation at the backup operational site.
- ✓ Facilitate effective co-ordination of recovery tasks and reduce the complexity of the recovery effort.
- ✓ Emergency response procedures within the event of fireside, flood disaster, civil disorder, natural disasters, bomb threats or the other incident or activity that will endanger lives, property or impede the capability to perform essential functions.
- ✓ Premises and essential equipment back-up and recovery.
  - ✓ Institutionalise disaster recovery process and procedures.

This DR Plan documents the IT Recovery Plan in sections with additional appendices and related documents required to support the Plan. Sections in this plan are organised as follows:

SECTION 1 – PLATFORM-SPECIFIC INFORMATION

This section contains platform specific information for each platform related to the Recovery Plan and includes the scope of the Recovery Plan, the assumptions made in its development and the critical applications, and their recovery time frames. It also includes an Escalation Plan for the Recovery Plan.

SECTION 2 – TEAM AND RESPONSIBILITIES

This section contains a description of the recovery team structure, members and their Disaster Recovery responsibilities.

SECTION 3 – BACKUP PROCESS

This section documents the backup process for the Disaster Recovery Plan. It contains current information and inventories of hardware, software, configurations, application backup procedures, and special inventories of off-site resources.

SECTION 4 -- RECOVERY PROCESS

This section contains the recovery process for the different platforms. The recovery process description includes notification, assessment, declaration, hardware, software, communications, and applications recovery. The section refers to the specific platform recovery procedures and contact information for internal and external resources.

SECTION 5 -- RECOVERY PLAN TESTING

This section contains information regarding the test process and schedule for the Recovery Plan.

SECTION 6 -- RECOVERY PLAN MAINTENANCE

This section contains information on the maintenance requirements and procedure for maintaining the Recovery Plan.

APPENDICES -- The appendices contain additional information to support the Disaster Recovery Plan.

1.2 DR DOCUMENTATION LOCATION

In order to allow IT employee to become familiar with the Recovery Plan, all the sections of the Recovery Plan and the procedures developed will be stored on the shared drives and on the COGTA intranet and a copy at the DR host site.

1.3 SCOPE

This Disaster Recovery Plan will in the event of a disaster cater for the IT infrastructure under the control of the IT section. Within the scope of this document is the recovery of the SQL server, the intranet, Teammate, Print Server (Y-Soft), File Server, AD Connect and all other database applications at the department.

This DR Plan addresses the following areas:

- ✓ Backup Process
- ✓ Recovery Process
- ✓ Plan Testing
- ✓ Plan Maintenance

1.4 ASSUMPTIONS

This Recovery Plan is developed and maintained based on the following assumptions:

- ✓ The Plan is designed to recover from all types of disasters including a worst-case situation; that is, all equipment, electronic files, procedures and documentation, and the computer room are not usable. It has also been assumed that the disaster will occur after hours. A disaster of lesser impact, or one that occurs during working hours should be dealt with by executing the relevant aspects of the recovery plan.
- ✓ That there is an expectation that recovery efforts can be executed within a realistic timeframe without excessive delays.
- ✓ Management intervention will determine which applications will be given restoration priority, based on the situation at the time of the disaster.
- ✓ That backups will be done according to the schedule defined in section 3 and will be rotated to off-site storage.
- ✓ That the level of Plan detail is based on the premise that sufficient and knowledgeable employees with similar skills will be available and can execute recovery actions.

UL

- ✓ Those off-site backup items are in a secure, environmentally protected and controlled facility sufficiently remote to the Head Office building not to be affected by the same interrupting event.
- ✓ That the critical employees will be able to use private transport to reach the recovery site.
- ✓ That essential resources (capital, personnel, technology) can be mobilized when needed.

1.5 ESCALATION PLAN

1.5.1 Escalation Plan Overview and Objectives

The Recovery Plan, though designed to get over a worst-case interruption, provides for the recovery from a minor to a significant outage, since minor to intermediate outages are way more common.

Declaring a DISASTER, leading to off-site recovery, is costly, time-consuming and very extremely disruptive. Thanks to the potential variables of a stoppage, including the time to repair/replace, GICTM must be prepared to create a **"GO"** or **"NO GO"** disaster decision within the critical time-frame.

Therefore, the objectives are:

- ✓ To define three escalation status levels that describe a minor, intermediate, or major interruption.
- ✓ To specify the timeframe after an intermission within which the disaster declaration decision must be made.

1.5.2 Escalation Plan Defined

The Escalation Plan deals with minor, intermediate, or major interruptions (or time windows) as defined below. Time windows are based upon the recovery time objective of 24 hours and a recovery point objective of 24 hours (maximum data loss of one day).

Specific tasks correspond to every Escalation Status. Status one and two relate to restoring computer services at the present site. Status three relates to a significant interruption and will probably finish during a disaster decision, initiating recovery at the recovery site.

ESCALATION STATUS ONE: "PROBLEM"

This is declared if the interruption is estimated to be **less than 24 hours**. The following steps will be taken in evaluating the escalation status:

- ✓ **Assessment**: Continuously monitor the situation to determine if the interruption will extend beyond 24 hours.
- ✓ **Modification**: If it becomes clear that the interruption will last more than 24 hours, modify the scheduled workload to prioritize critical application systems.
- ✓ **Restoration**: Begin restoring system programming and production application data as needed.
- ✓ **Vendor Assistance**: Ensure that vendors are on standby to provide necessary support.
- ✓ **Declaration**: Officially declare the transition to "EMERGENCY" status.

ESCALATION STATUS TWO: "EMERGENCY"

This is declared if the interruption is estimated to be **more than 24 hours and fewer than 48 hours.** Modifications are going to be made to the scheduled workload to allow the best priority application systems to run as soon as possible. Looking on the extent of harm, some restoration of system programming and production application data are performed. Most applications will run at normal levels following the restoration and recovery process. Corrective action by the support employee is also necessary. The following steps will be taken in evaluating the escalation status:

- ✓ **Assessment**: Continuously monitor the situation to determine if the interruption will extend beyond 48 hours.
- ✓ **Mobilization**: Prepare the Disaster Recovery Teams for full mobilization.
- ✓ **Recovery Facility**: Arrange for the systems to be recovered at the designated recovery facility.
- ✓ **Vendor Assistance**: Ensure that vendors are fully engaged and providing necessary support.
- ✓ **Declaration**: Officially declare the transition to "DISASTER" status and assert the whole building as being in Recovery Mode of operation

ESCALATION STATUS THREE: "DISASTER"

This is declared if the interruption is estimated to be **48 hours or more**. The systems are going to be recovered at the recovery facility. Full mobilisation of the Disaster Recovery Teams is required. During this status of the escalation plan, the whole building is asserted as being in Recovery Mode of operation.

Communication: Maintain clear and constant communication with all stakeholders, including support employees, vendors, and recovery teams.

Documentation: Keep detailed records of all actions taken, decisions made, and the current status of the recovery process.

Coordination: Ensure that all teams are coordinated and aware of their roles and responsibilities during each escalation status.

Review: Regularly review the situation and adjust the recovery plan as needed to address any new challenges or changes in the situation.

1.6 RECOVERY REQUIREMENTS

Based on the analysis carried out by GICTM, recovery objectives have been established for critical systems and applications. These objectives range from 1 to 3 days, depending on the recovery priority assigned to each system, as detailed in Section 3 of the System and Application Inventory and Priority. In the event of a major IT service interruption, a more granular prioritisation may be necessary, requiring management involvement to determine the precise order of recovery.

1.7 RECOVERY STRATEGY

The recovery strategy is a statement of intent. It explains how GICTM has planned to deal with Disaster Recovery.

The disaster recovery site for the restoration of the systems is at: COGTA, Old Ford House, Sarah Baartman District.

The department has servers configured on site for back-ups and replication.

The following systems and Applications will be recovered:

- SQL server, the intranet, Teammate, Print Server (Y-Soft), File Server, AD Connect and all other database applications at the department.

The department currently utilises an on-prem backup solution. In the event of a disaster, it would be necessary to recover the servers using these backup and replication storage media.

The Backup & Replication software the department utilises allows:

- Immediate recovery of a failed VM, thus reducing downtime of production VMs to the minimum (Instant VM Recovery).
- Verification of recoverability of every backup by starting and testing VMs directly from VM backups in an isolated environment.
- Restore items from any virtualized applications with Veeam Explorers.
- Restore guest OS files with Multi-OS File-Level Recovery.

2 TEAMS AND RESPONSIBILITIES

The Recovery Team is made up of one main functional area, which consists of one recovery team. The Disaster Recovery Co-ordinator is responsible for communicating with management and eliminating roadblocks facing the Recovery Team during the recovery process. The co-ordinator of the Recovery Team will continually report the status of the recovery to the DR leader , while the team performs the detailed tasks necessary to perform the recovery and return to normal operations.

The DR co-ordinator and Recovery Team responsibilities are listed here. These responsibilities are broken down into categories of what to do before, during, and after a disaster.

2.1 RECOVERY TEAMS

The recovery teams are responsible for the recovery of the services offered by GICTM. It is the responsibility of the recovery team leaders to see that the team responsibilities outlined in this section are carried out, either by the team leaders themselves or by team members

2.1.1 Recovery Team Leader's Contact Details

Role	Name	Contact Details
Recovery Team Leader	Tswakai Luke	**(Cell) 076 141 1749**

2.1.2 DR co-ordinator's Contact Details

Role	Name	Contact Details
DR Co-ordinator	Mawethu Damane	**(Cell) 082 798 3604**

DR Co-ordinator	Thembela Mngaza	**(Cell) 076 819 5221** **(Cell) 060 977 5603**
DR Co-ordinator	Lamantambo Ndadana	**(Cell) 072 426 7974**

2.2 DR CO-ORDINATOR

The DR Co-ordinator is responsible for overseeing the entire recovery operation.

Charter: Restore critical IT systems at the recovery site.

Pre-Disaster Responsibilities

- ✓ Establish, document, and maintain system backup and recovery procedures.
- ✓ Document and maintain current system configuration diagrams, hardware and software inventories, and vendor contacts.
- ✓ Review the recovery facility documentation and manuals.
- ✓ Ensure that all vital records are stored at the off-site storage facility.
- ✓ Cross-train team members and test recovery procedures regularly

Disaster Responsibilities

- ✓ Respond immediately to a disaster alert.
- ✓ Review the status of systems and prepare a report for the Damage Assessment Meeting.
- ✓ Mobilize the recovery team and contact alternate or substitute team members as needed.
- ✓ Ensure all manuals, documentation, and backup media are available at the recovery facility.
- ✓ Work with vendors and the DR Coordinator to confirm the required equipment upgrade and installation

Post-Disaster Responsibilities

- ✓ Perform an assessment of team effectiveness during the disaster.
- ✓ Modify team tasks and procedures as required.
- ✓ Assess performance in recovery mode and make recommendations.
- ✓ Assess effectiveness of the Recovery Plan for your area of responsibility.
- ✓ Revise and update existing procedures

2.3 RECOVERY TEAM

Charter: Restore and support the impacted IT systems.

Pre-Disaster Responsibilities

- ✓ Establish, document, and maintain system backup and recovery procedures.
- ✓ Document and maintain the currency of network backup and recovery procedures, configurations, and all pertinent network information.
- ✓ Ensure that all vital records are stored at the off-site storage facility.
- ✓ Test recovery procedures and evaluating test results

Disaster Responsibilities

- ✓ Respond immediately to an invitation from the DR Team Leader.
- ✓ Notify the resources required for network recovery.
- ✓ Meet at the recovery site and review the current disaster situation, recovery procedures, and roles and responsibilities.
- ✓ Ensure all manuals, documentation, and backups are available.
- ✓ Provide the mandatory network connectivity and work with SITA Networks to determine full network connectivity
- ✓ Restore systems using the defined recovery procedures.
- ✓ Provide the DR Co-ordinator with ongoing status and notification of system availability

Post-Disaster Responsibilities

- ✓ Perform an assessment of team effectiveness during the disaster.
- ✓ Modify team tasks and procedures as the circumstance arises.
- ✓ Assess performance in recovery mode and make recommendations.
- ✓ Revise and update existing procedures

3 BACKUP PROCESS

The purpose of this section is to tabulate the backup measures for system recovery and network connectivity. This section covers the areas of the backup process and facilities, and the resources and facilities related to recovery.

3.1 INVENTORY

This section of the Recovery Plan provides inventories of the assorted aspects of system hardware, software and data. The backup system follows a grandfathering approach. A full system backup is done every week and incrementally daily.

3.1.1 Backup Inventory

This section deals with the present backup process for the computer programmes, applications, and data. The Backup & Replication software provides a set of features for building and maintaining a flexible backup infrastructure, performing data protection tasks (such as, regular backup and replication of VMs and Physical Servers), and carrying out disaster recovery procedures.

3.1.2 Back-up Schedule

The following systems are backed up and replicated:

- ✓ Microsoft SQL Server 2014
- ✓ Print Server (Y-Soft)
- ✓ Teammate Server (Internal Audit system)
- ✓ File Server
- ✓ Active Directory Connect & Active Directory - (Identity Management)
- ✓ Intranet Server
- ✓ GIS Server

3.1.3 Backup & Replication

Backup & Replication is an availability, data protection and disaster recovery solution for VMware vSphere and Hyper-V virtual environments of any size and complexity.

To provide the most comprehensive protection of the department virtual infrastructure, Veeam Backup & Replication complements image-based backup with image-based replication. Veeam can back up any VM, VM container or VM disk, as well as replicate VMs onsite for high availability (HA) or offsite for disaster recovery (DR), across local area and wide area networks.

The Backup & Replication software offers technology that allows you to:

- ✓ Immediately recover a failed VM, thus reducing downtime of production VMs to the minimum (Instant VM Recovery).
- ✓ Verify recoverability of every backup by starting and testing VMs directly from VM backups in an isolated environment.
- ✓ Restore items from any virtualized applications with Veeam Explorers and U-AIR .
- ✓ Restore guest OS files with Multi-OS File-Level Recovery.

3.1.4 Backup Proxy (Hyper-V)

By default, when you perform backup, replication or VM copy jobs in the Hyper-V environment, VM data is processed directly on the source Hyper-V host where VMs reside and then moved to the target. However, VM data processing can produce unwanted overhead on the production Hyper-V host and impact performance of VMs running on this host. To take data processing off the production Hyper-V host, the off-host backup mode can be used.

3.1.5 System and Application Inventory and Priority

The list of systems and applications and the associated recovery requirements are tabled below.

3.1.6 Systems

System recovery within	Number of systems	Total Gigabytes
12 hours	8	10.43TB

Systems are to be recovered within 12 hours.

System description	Department/User	Size	Restore time in hours
Microsoft SQL Server 2014	GICTM	180GB	8
Print Server (Y-Soft)	GICTM	260GB	6
Teammate Server (Internal Audit system)	GICTM	93GB	6
File Server	GICTM	8.5TB	8
Active Directory - (Identity Management)	GICTM	72.5GB	8
Intranet Server	GICTM	780GB	8
GIS Server	GICTM	350GB	8
Active Directory Connect	GICTM	195GB	8

These 8 systems/databases represent approximately 10.43TB.

3.1.7 Hardware Inventory

These are the physical servers:

SERVERS
GIS SERVER
HOST 1 (HV01)
HOST 2 (HV02)
HOST 3 (HV03)
HOST 4 (HV04)
BACKUP REPOSITORY
VEAAM HOST
REPLICATION SERVER (SARAH BAARTMAN)
RESTORE SERVER (SARAH BAARTMAN)

The following servers are all Virtual Machines that are hosted on the following hosts:

VM's	HOSTS
File server	ALL VMs HOSTED ON THE CLUSTER, EXCEPT:
Teammate	
Microsoft SQL Server 2014	
Print Server (Y-Soft)	
File Server	
Active Directory Connect	
Intranet Server	
Active Directory - (Identity Management)	HVO4

3.1.8 Equipment and supplies needed for backup.

The following is needed to perform a backup:

- ✓ Storage device
- ✓ Backup server

The following is needed to perform replication.

- ✓ Storage device
- ✓ Replication server

3.2 OFF-SITE REPLICATION

The replication server will be kept in the Sarah Baartman DSC Office because it is government-owned, unlike the privately-owned Amatole DSC office.

3.3 RECOVERY SITE

Alternate recovery site shall be situated in an exceedingly location a minimum of "100KM" ([10/50/100]) away from primary site Bhisho not sharing common natural disaster types. Every effort is made to ensure that a replica site is not served by the same utility and communication providers as the primary site. In cases where the same providers are utilized, it must be demonstrated that adequate redundancy exists to avoid dependence on the same telecommunication and electricity lines.

Noting the current IT WAN structure, Sarah Baartman DSC in Gqeberha is deemed the alternate recovery site utilizing the upgraded bandwidth through Provincial Broadband Project. The recovery site will be used to support a server virtualisation solution, network connectivity and printing capability until it is possible to return to the COGTA premises in Bhisho. The recovery site is also used to house the DR materials and software that GICTM would need for recovery in the event of a disaster.

Directions to the recovery site:

Take the N2 towards **Gqeberha**, Exit onto **Albany Road**. At the **second set of traffic lights (robots)**, turn right into **Westbourne Road**. Immediately turn **right** again into **Clevedon Road**. Continue towards the **Old Ford Building**, which houses the **CoGTA Sarah Baartman DSC offices**. Locate the server room on the **first** floor of the building.

Remember that to declare a disaster or to place the recovery site on standby, the Disaster Recovery Co-ordinator must be involved.

4 IT RECOVERY

This section of the Recovery Plan describes the restoration of the IT environment.

4.1 INVOKE DISASTER RECOVERY

This section identifies the activities from disaster declaration, up to the recovery of the systems at the recovery site. The DR Co-ordinator is responsible for these activities, including their delegation.

4.1.1 DR Actions to be followed:

	Action Description	Time	Responsible Person Initials	Comments
NB!! • **This table needs to be used as a worksheet during testing or disaster recovery.** • **Any changes/additions will be appreciated.** • **Time and Comments will be used for minutes and reporting.** • **An Event Log needs to be kept by the Co-ordinator during the recovery process –**				
1.	Receive disaster alert. Wait for further notification.			
2.	Optional: Phone team members to place them on alert for possible callout. Contact information can be found in APPENDICES			
3.	Receive information that a disaster has been declared. Ensure that you understand what is required.			
4.	Determine which strategy required for recovery.			
5.	Submit Subnet relocation forms to SITA/OSIS. Contact information can be found in APPENDICES			
6	Contact team members and ask them to proceed to recovery site. Ensure that they know how to get there. Contact information can be found in RECOVERY SITE			
7.	Arrival and registration at recovery site.			
8.	Recovery Team to obtain the checklist to start the necessary arrangements. Refer to DR CO-ORDINATOR			
9.	Check the backup and replication infrastructure on arrival.			
10.	Check the configuration of the equipment.			
11.	Contact vendors and DBA's to provide necessary support if required.			
12.	Wait for Network Recovery Team's (SITA/OSIS) notification that network is available.			Server OS installation and Restores can begin without the network in place
13.	Start recovery of servers			
14.	Contact System DBA to verify contents of the databases.			
15.	Wait for notification to switch the network to go live.			
16.	Arrange for a complete backup that is to be stored off-site.			
17.	Inform Co-ordinator about completion of the recovery.			
18.	Co-ordinator to collect all worksheets and Event logs for			

	Action Description	Time	Responsible Person Initials	Comments
	the purpose of reporting.			
17.	Users to proceed with business as usual.			
18.	All teams to be on standby for support as users start using the systems.			

4.2 PREPARE ENVIRONMENT

Check that the recovery room at the recovery site is adequately equipped. Any problems encountered should be reported to the DR Co-ordinator.

The Recovery Team must involve SITA Networks, if they have not already been contacted to restore network connectivity.

4.3 RECOVER SQL SERVER

The network administrator must have proper arrangements to save the databases from any kind of loss in case of such by conducting the following:

- Taking database backup regularly
- Fail-over clustering instances that facilitate server protection from unexpected damage or failure
- Database replication procedure which involves copying SQL Server database and distributing it to another database.

4.4 RECOVERY RESOURCES

The basic recovery resources needed by the recovery teams are listed below. These resources have been lodged at the recovery site wherever possible.

Inventory Items for the Server Room that will need to be restored in the event of a disaster.

Manufacturer	Description
DELL Server X 2	Power-Edge R530
EMC storage	1 SAN storage
Server Racks	For hosting the EMC server

Manufacturer	Description
Cisco switches	3 Cisco 2960-X Switches
UPS	1 Power Supply
KVM	Keyboard, Video, Monitor system
Air conditioner	Server room environmental controls
Telephones (Cell phones)	Communication tool
Disaster Recovery Plan	Plan that documents steps to be taken during disaster

5 DR TEST PROCESS

The purpose of this chapter is to stipulate the method for testing the Recovery Plan. The recovery plan is tested to make sure that the documented recovery process and associated procedures are executable and accurate. After each test has been conducted an evaluation of the test must be performed. The evaluation should judge a test on its productivity toward recovery, as opposed to recovery success alone.

In addition, this section explains the method that ought to be followed for planning, conducting, and reviewing tests.

5.1 SCHEDULED TESTS

A preliminary schedule should be developed for the year(s) ahead. This schedule will assist in allocating the specified budget, employee planning (shifts, leave etc.) and might be used to provide Management with the status of recovery planning supported the results of previous test(s) and those planned.

DATE	DURATION	SCOPE

Table 5.2 – Scheduled Tests

5.2 PRE-TEST PLANNING

As explained earlier, conducting a recovery test affects the assembly environment, and may be a costly exercise for the GICTM. So as to get maximum value from the test, planning must be thorough and may be completed within a minimum of 3 weeks before the date of the test. This section outlines the areas that pre-test planning should consider.

5.2.1 Objectives

Clearly defined objectives are essential for the test. If previous tests have been conducted, future objectives may differ as processes become more efficient. The Test Co-ordinator will use these objectives to guide the planning, execution, and evaluation of the test. It is helpful to distinguish between primary objectives, which are necessary for the test to be deemed successful, and secondary objectives, which can be achieved if circumstances allow.

Possible objectives may include some, all or a mix of those examples:

- ✓ Verify the accuracy of the plan.
- ✓ Verify the accuracy of the procedures.
- ✓ Give a wider cross-section of employee experience in DR testing
- ✓ Recover within the shortest possible time.
- ✓ Recovery with a focus on a particular component, which may have been a problem area in previous tests
- ✓ Record the timeframes of individual activities.

5.2.2 Test Guidelines

The objectives may be expressed in terms of **Test Guidelines**. These guidelines are developed to support the basic objectives of the test. The guidelines will be enforced by the Test Co-ordinator and will be used as a basis for test planning. Some examples of guidelines are:

- ✓ Working hours
- ✓ Work instructions such as recording task duration, missing documentation etc.
- ✓ An escalation procedure that should be followed in the event of difficulties with the recovery process or the recovery site

The **scope** of the test must be well defined, as dictated by the objectives of the test. This must be done in order for any further planning to be done.

Any **assumptions** that are made regarding the test must be documented so that the participants in the tests are aware of them and can react accordingly if these assumptions prove to be incorrect.

5.2.3 Participants

The individuals that will participate in the test must be identified, and their responsibilities discussed, agreed, and formally assigned. Since this will have an impact on the provision of day-today support, planning is vital. This also allows Management to cater for employee availability, requests for leave, courses etc.

Not all participants in the test may be required to travel to the recovery site. If people that remain at the production site are required to participate in the test, this should be specified as well. The role of the employee at site could range from providing telephonic assistance if required, to being actively involved in verification testing after hours.

5.2.4 Logistics

The logistic planning for a test can affect the ability of the individuals involved to successfully execute the test. This is an area that must be dealt with well in advance. Planning will also allow all relevant regulations to be followed without compromise. In addition, the recovery site may want to follow a process that allows the site to be prepared for the test.

There are several aspects that must be considered while making the logistic arrangements for a test. Each task must be assigned to an individual with an expected completion date. Some of the key areas are:

- ✓ Reservation of the recovery site
- ✓ Bookings for food and accommodation (depending on the location of the recovery site).
- ✓ Directions to the recovery site and place of accommodation
- ✓ Payment for food, accommodation, overtime, and other related expenses

- ✓ Transport arrangements
- ✓ Consumables (notepads, pens, print material, scratch tapes etc.)
- ✓ Backups availability and access to general facilities
- ✓ Reference materials

5.3 TESTING PROCESS

The activities that will be executed during the test must be clearly specified. This will allow the participants to prepare for the test and raise any concerns or queries prior to the test. The Recovery Plan and recovery procedures must be referred to, with a description of which aspects of the Recovery Plan should be executed during the test, if only parts of the plan are needed for a specific test.

Additional activities (those activities not covered in the Recovery Plan that are relevant to the testing process) must be included and assigned to specific individuals or teams. One example of an activity that may have to be specified is informing the users if the test includes network switching or downtime (e.g. Full Interruption Test).

List of Disaster Recovery Tests to choose based on appropriateness

DR Test	Description	Testing Frequency
Checklist Review	✓ A simple review of the DR plan to ensure all components are up to date. ✓ **Low cost, low effort**	Every **6 to 12 months**
Tabletop Exercise	✓ Stakeholders walk through the DR scenario in a meeting setting. ✓ **Good for identifying gaps in communication and procedures.**	
Simulation Test	✓ A simulated disaster scenario is created to test responses. ✓ **Tests coordination and decision-making.**	Annually or **after major system changes**
Parallel Test	✓ Systems are restored at an alternate site without disrupting production. ✓ **Validates recovery procedures without risk to operations.**	
Full Interruption Test	✓ Production systems are shut down and recovery is performed. ✓ **High risk but provides the most realistic test.**	Every **2 to 3 years**, if feasible

5.4 POST-TEST PROCESS

The testing process does not end with the execution of the DR test. In order to achieve the full benefit of the exercise, the process must be reviewed.

After a disaster recovery (DR) test is conducted, post-test processes are essential to evaluate the effectiveness of the test and improve future responses. This section explains the key activities that should be considered after a test are as follows:

- ✓ **Test Review and Debriefing** : How it's done: All stakeholders (IT employee, management, vendors) meet to discuss what happened during the test. The aim is to identify what worked, what didn't, and any unexpected issues.
- ✓ **Documentation of Results** : How it's done: Detailed records are created, including timelines, system performance, recovery point objectives (RPO), and recovery time objectives (RTO). The aim is to provide a factual basis for analysis and future reference.
- ✓ **Gap Analysis :** How it's done: Compare actual outcomes with expected outcomes. The aim is to identify discrepancies, such as systems that took too long to recover or data that was lost.
- ✓ **Corrective Actions :** How it's done: Implement changes to address issues found during the test. The aim is to strengthen the disaster recovery plan (DRP) and infrastructure.
- ✓ **Plan Updates :** How it's done: Update the DRP documentation to reflect lessons learned and new procedures. The aim is to ensure the plan remains current and effective.
- ✓ **Stakeholder Communication :** How it's done: Share findings and updates with all relevant parties. The aim is to maintain transparency and ensure everyone is aligned.

5.4.1 Post-Test Activities

Any activities that must be carried out after the test is completed must also be listed. Like testing activities, these tasks must be assigned to individuals.

This could include activities such as the following:

- ✓ Returning any equipment borrowed from a vendor
- ✓ Replacing materials taken from the production environment (manuals, CDs etc.) □ Returning the off-site backups to their proper place
- ✓ Debriefing Session: Review what happened, what went well, and what challenges were encountered.
- ✓ Performance Evaluation: Compare actual recovery times and data integrity against Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

Uh

- ✓ Incident Documentation: Log all actions taken, issues encountered, and outcomes achieved.
- ✓ Gap Analysis: compare expected vs. actual results to find discrepancies.
- ✓ Feedback Collection: Use surveys or interviews to gather insights on the test experience.
- ✓ Corrective Action Planning: Develop and assign tasks to fix problems or improve procedures.
- ✓ Plan and Policy Updates: Revise documentation, contact lists, procedures, and infrastructure details.
- ✓ Reporting to Management: Prepare a summary report with findings, recommendations, and next steps.
- ✓ Archiving Test Results: Store all documentation securely and accessibly.
- ✓ Scheduling the Next Test: Plan the next test based on risk, system changes, or compliance needs.

5.4.2 Review Meeting

A post-test meeting with the recovery team should be held after the test, chaired by the Test Coordinator. The objective of this workshop is to conduct a detailed review of the test. This feedback will allow the recovery site to be better prepared for future tests and will also allow the recovery teams the opportunity to learn from the experience.

The recovery site employee should also provide feedback to the Test Co-ordinator on their observations during the test and pass on any suggestions for improvement if applicable.

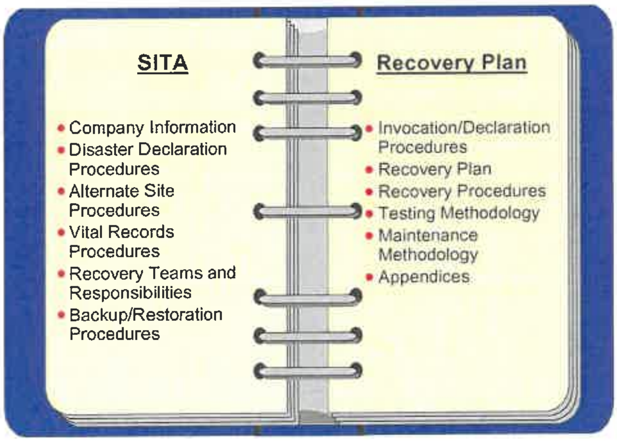
- ✓ All problems experienced during the test must be discussed with the following objectives:
- ✓ Understand and agree on what the actual cause of the problem was
- ✓ Decide what will be done about the problem (change backups, modify plans and procedures etc.)
- ✓ Decide who will execute this change and when it will be done
- ✓ During the workshop, the information gathered will be used to prepare the Test Evaluation Report. This report will used to document the result of the test, and the corrective actions that will be taken in reaction to the problems encountered. It will be

the responsibility of the Test Co-ordinator to document and circulate the Test Evaluation Report to employee and Management as appropriate.

The major areas of the Test Evaluation Report are as follows:

- ✓ Test Details (date, duration, participants etc.)
- ✓ Executive summary (for Management to get an overview of the test)
- ✓ Evaluation of each area of the test against the defined objectives and guidelines.
- ✓ Servers
- ✓ Network
- ✓ Operations
- ✓ Evaluation of the recovery site

6 DR MAINTENANCE PROCESS


SITA
• Company Information
• Disaster Declaration Procedures
• Alternate Site Procedures
• Vital Records Procedures
• Recovery Teams and Responsibilities
• Backup/Restoration Procedures
Recovery Plan
• Invocation/Declaration Procedures
• Recovery Plan
• Recovery Procedures
• Testing Methodology
• Maintenance Methodology
• Appendices

The purpose of this section is to define the activities necessary to maintain the Recovery Plan. Plan maintenance is of utmost importance to assure currency of what is to be recovered, and the procedures governing the recovery. This means keeping the test plan current and synchronised with changes. All changes in both the production and work environments must be considered when updating the Recovery Plan.

6.1 RESPONSIBILITIES

The Maintenance approach adopted for the DRP is that of co-sourcing. This means that the Disaster Recovery Project Team will assist in the maintenance of the Recovery Plan and related documentation. The responsibility to notify the DR Team of changes that need to be made to the documentation lies with the GICTM. The DR Team is responsible for modifying the affected documents with the changes requested by the GICTM.

The information that will need to be updated falls into one of 2 categories, Production Environment Information or Work Environment Information. The Production Environment Information deals with the IT infrastructure, which includes any aspect of mainframe or network operations. The Work Environment Information deals with changes to the IT section and their working environment.

6.2 MAINTENANCE MECHANISM

The recovery documentation will be updated monthly to review all changes that have been implemented or are scheduled for implementation in the production environment. The monthly review will also be the opportunity for changes to the Recovery Plan to be requested.

7 APPENDICES

7.1 EMPLOYEE CONTACT DETAILS

EMPLOYEE CONTACT LIST

Name	DR Role(s)	Home Tel.	Work Tel.	Cell.
DISASTER RECOVERY CO-ORDINATOR				
Mawethu Damane	Deputy Director: Infrastructure		040 940 7243	082 798 3604
Thembela Mngaza	Network Administrator		040 609 5496	072 751 6298
Lamantambo Ndadana	LAN/Network Technician		040 609 7441	072 426 7974
RECOVERY TEAM LEADER				
Tswakai Luke	Director: GICTM	0437400450	0409407235	083 459 7919 076 141 1749
Sisanda Brukwe	Deputy Director: Operations		0409407242	071 602 1033
RECOVERY TEAM				
Vuyo Mlokothi				072 903 9833
Dr. Siviwe Mditshwa			040 940 7674	066 381 0716

8 REVIEW OF THE PLAN

The plan will be reviewed every five (5) years from date of approval and when there are material changes in the enabling legislation or the operating environment.

lv