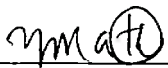





**LIMPOPO GAMBLING BOARD  
INFORMATION TECHNOLOGY UNIT**

# **LGB Disaster Recovery Plan**

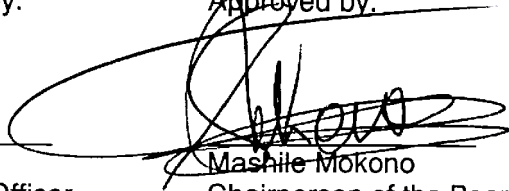
Prepared by:

  
Yvonne Mathabatha  
Chief Financial Officer

Recommended by:

  
Serobi Maja  
Chief Executive Officer

Approved by:

  
Mashile Mokono  
Chairperson of the Board

Version	April 2016	
Effective date		

## **FOREWORD**

This is a disaster Recovery Strategy report for the Limpopo Gambling Board. The purpose of the disaster Recovery Strategy was to identify threats and vulnerabilities in relation to the IT Unit of the Limpopo Gambling Board and develop strategies on how to continue with the business when those identified threats are realised.

# **CONTENTS**

<b>LGB Disaster Recovery Plan .....</b>	<b>1</b>
<b>FOREWORD .....</b>	<b>2</b>
<b>1 Background .....</b>	<b>4</b>
<b>2 IT Systems.....</b>	<b>4</b>
<b>3 Benefits of disaster recovery plan .....</b>	<b>5</b>
<b>4 Developing a disaster recovery plan .....</b>	<b>5</b>
4.1 Planning areas.....	5
4.2 Sections of the plan .....	5
4.3 Ownership, change and version control .....	6
4.3.1 Designated plan owner .....	6
4.3.2 Access to and users of the plan.....	6
4.3.3 Management signoff of the plan .....	6
4.3.4 Accountable managers.....	6
4.3.5 Version and change control of the plan .....	6
4.3.6 Recovery information roles and responsibilities .....	7
<b>5 Recovery scenarios.....</b>	<b>7</b>
5.1 Scenario 1: minor damage.....	7
5.2 Scenario 2: major damage.....	8
<b>6 Disaster recovery processes .....</b>	<b>8</b>
6.1 Reporting the incident .....	9
6.2 Incident reporting .....	9
6.2.1 Assessing the incident .....	10
6.2.2 Incident management team.....	10
6.2.3 Damage assessment procedures .....	10
6.2.4 Damage Assessment Checklist .....	11
6.2.5 Escalation .....	13
6.2.6 Crisis Management Team .....	13
6.2.7 Disaster Declaration Authority .....	14
6.2.8 Designated authorities who may declare a disaster.....	14
6.2.9 BCMT/ITRT team.....	14
6.3 Recovery phase .....	15
6.3.1 DR briefing and analysis of the damage assessment .....	16
6.3.2 Invoke recovery procedures .....	16
6.3.3 Backup personnel contact details .....	16
6.4 Return to normal phase .....	16
6.4.1 Information requirements.....	17
6.5 Damage assessment and salvage team .....	18
6.5.1 Damage assessment and salvage team responsibilities .....	18
6.6 Physical security team .....	18
6.6.1 Physical security team responsibilities.....	18
6.6.2 Communications team responsibilities.....	19
6.6.3 Hardware installation team responsibilities .....	19
6.6.4 IT recovery team responsibilities.....	19
6.6.5 IT technical team responsibilities.....	19
6.6.6 Asset replacement procedures .....	20
6.6.7 Damage assessment checklist.....	20
6.6.8 Disaster recovery plan maintenance .....	20
6.6.9 Disaster recovery plan testing.....	21
<b>Annex A. Acronyms .....</b>	<b>23</b>

## **Background**

Limpopo Gambling Board (LGB) is increasingly dependent on information and communication technology to operate effectively and efficiently. Information is therefore as valuable an asset to the LGB as any other physical asset or intellectual property owned and produced by the LGB. IT systems are vulnerable to a variety of disruptions ranging from mild disruption such as disk drive failures to severe disruptions such as the destruction of equipment or fires. Vulnerabilities may be minimized or eliminated through technical, managerial or operational solutions as part of the LGB's risk management effort. It is however virtually impossible to completely eliminate all risks. Contingency planning is designed to mitigate the risk of system and service unavailability by focusing on effective and efficient recovery solutions. It is vital for the LGB to have a proper disaster recovery plan in place.

This disaster recovery plan outlines the nature and location of LGB systems and the necessary actions required to ensure that it will be able to resume normal business function (or as close to it as possible) in the event of a disaster occurring as a result of whatever cause, whether storm, fire, natural disasters or malicious attacks intending to destroy organizational information and systems. The IT function of the LGB is focused on ensuring that vital assets are restored to working order as quickly as possible as failing to do so may hamper the goal of the LGB of providing efficient and effective services to the South African public. It is therefore the intention of the LGB to comply with industry best practices, international standards and corporate governance regulatory requirements for developing and maintaining business continuity and that best meet the needs of the government.

## **2 IT Systems**

This plan will guide the LGB through the many activities associated with achieving its recovery objectives. It assumes that recovery team participants have a reasonable knowledge of LGB business processes and had formal training in the various computing disciplines applicable to their respective areas.

No.	server	Proprietary/ open source	Application	Location	Priority
1	Financial system server (Lgbsrvfin01 and srv-02)	Windows 2008	VIP, E-SS,HR Accpac, and D-bit	LGB	One
2	Mail Server (lgbsrvexch01)	Windows 2012	MS outlook	LGB	One
3	Domino server (NS5)	Windows 2003	Lotus notes	LGB	Two
4	File server (NS3)	Windows 2008	N/A	LGB	Two
5	Domain controller(Lgbsrvdc01) and Lgbsrvdc02)	Windows 2012	N/A	LGB	One
6	Managed by Bluecameleon/Limitech	Linux	TMS	LGB	Three

**Table 1: IT Systems**

### **3 Benefits of disaster recovery plan**

Developing a disaster recovery plan will;

- a) provide the LGB with a sense of security;
- b) minimise the risk of delays;
- c) guarantee reliability of standby systems;
- d) provide a standard for testing the plan;
- e) establish a DR team to manage disasters;
- f) coordinate recoveries, ensure business continuity and protect LGB systems from major disruptions or disasters;
- g) address the recovery of resources, products and services following a disaster within the computer room or on the network affecting LGB systems;
- h) determine the events that can adversely affect the effective functioning of LGB systems and the damage from such events, the time scale needed to restore normal operations and the controls that can be implemented to reduce the impact

### **4 Developing a disaster recovery plan**

#### **4.1 Planning areas**

Various scenarios that forms the basis of the plan was considered and a multitude of assumptions were made in the process.

The key principles the plan applies to are;

- a) critical unrecoverable hardware failures such as servers or switches;
- b) any computer room facilities or servers becoming inaccessible preventing the LGB from performing its normal operational functions;
- c) a predetermined disaster recovery site and IT resources that will be used to recover critical system functionality during an emergency that prevents access to any of the regional systems or servers

#### **4.2 Sections of the plan**

The DRP consists 4 main sections that are divided into subsections. Those are:

- a) DRP ownership, change and version control;
- b) the DRP strategy;
- c) the disaster recovery process; and
  - i) the alert phase;
  - ii) the recovery phase; and
  - iii) the return to normal phase

## 4.3 Ownership, change and version control

### 4.3.1 Designated plan owner

The DRP forms part of the overall LGB business continuity plan, but DRP still has its own designated owner. The owner of the plan is IT management. The DRP owner has to ensure that the correct recovery strategy is adopted.

The Limpopo Gambling Board management takes overall responsibility for the Plan in terms of;

- a) maintaining the plan e.g. regular updates that accurately reflect changes in the production environment should be done on at least a monthly basis;
- b) scheduled recovery tests that include specific recovery objectives for each test;
- c) correct and up-to date technical procedures;
- d) ensuring that the plan is reviewed when there are;
  - i) additions, deletions or upgrades to hardware platforms;
  - ii) additions, deletions or upgrades to system software;
  - iii) changes to system configuration;
  - iv) changes to application software;
  - v) changes that affects the availability of the disaster recovery facility;
  - vi) changes to staff identified by name in the plan;
  - vii) changes to off-site backup procedures;
  - viii) changes to application backups; and
  - ix) changes to vendor lists maintained in the plan

### 4.3.2 Access to and users of the plan

The plan contains confidential information. Uncontrolled access to the plan may lead to security breaches and business risks. A signed hard copy will be kept by the LGB CEO for security reasons and the other copy will be kept by the designated disaster recovery coordinator. Note that all printed copies of the plan, except the PDF master copy, are uncontrolled.

The plan and its contents would only be accessible to LGB staff members that play an active role in the recovery process. In terms of awareness to the rest of the organisation, a high-level overview of the plan will be made available for general perusal.

### 4.3.3 Management signoff of the plan

The Office of the CEO needs to take ultimate accountability for the information contained in the plan. Lack of managerial commitment may lead to recovery failure and ultimately a business risk.

### 4.3.4 Accountable managers

Name	Designation	Work Tel	Cell number
M. Lavhengwa	Manager	015 230 2322	082 904 4201
M. Mathabatha	Chief Financial Officer	015 230 2306	082 578 5978
K. Bidzha	IT Officer	015 230 2323	082 333 8084

Table 2: accountable managers

### 4.3.5 Version and change control of the plan

It is inevitable in the changing environment of the IT industry that this disaster recovery plan will become outdated and unusable unless someone keeps it up to date. Changes that will likely affect the plan fall into several categories. Those categories are;

- a) hardware changes;
- b) software changes;

- c) facility changes;
- d) procedural changes; and
- e) personnel changes

As changes occur in any of the abovementioned areas, the LGB IT business unit, through the designated disaster recovery coordinator will determine if changes to the plan are necessary. This decision will require that managers be familiar with the plan in some detail. The common changes that will require plan maintenance are listed in above.

The staff in the affected area will make changes that affect the platform recovery portions of the plan. After the changes have been made the LGB disaster recovery management will be advised that the updated documents are available. They will incorporate the changes into the body of the plan and distribute as required.

All updates or changes to the disaster recovery plan shall comply with the change control policy with regards to assessing if the change is necessary, validating the adequacy of the acceptance test, scheduling the promotion into a test environment, notifying the appropriate functions and verifying whether the change was implemented successfully.

### 4.3.6 Recovery information roles and responsibilities

Role	Responsibility
Disaster Recovery Coordinator K. Bidzha	Responsible for the implementation of the DRP, and overall compliance with, the Disaster Recovery Policy within their area of responsibility
IT Manager M. Lavhengwa	Communicate all decisions/upgrades/changes/new implementations in respect of technology that will directly impact disaster recovery capabilities and procedures to the Disaster Recovery Unit
IT Manager M. Lavhengwa	Compile and maintain, in accordance with standards, and with the assistance of the Disaster Recovery Unit, individual Disaster Recovery procedures and supply a copy thereof to the Disaster Recovery Unit
Disaster Recovery Coordinator K. Bidzha	Active involvement in disaster recovery tests and the production of a detailed test log.
Disaster Recovery Coordinator K. Bidzha	Provide a full consultation service on the compilation of individual Disaster Recovery Plans which includes: Brief Impact and Risk analysis

**Table 3: recovery information- roles and responsibilities**

## 5 Recovery scenarios

This section describes the various recovery scenarios that can be implemented, depending on the nature of a disaster and the extent of the damage. The Disaster Recovery Coordinator decides which recovery scenario to implement when the Disaster Recovery Plan is invoked.

### 5.1 Scenario 1: minor damage

In this scenario only a part of the computer processing environment may be affected, but the communication lines and network are still active. The goal of the recovery process in this case is to move the applications from unavailable systems to the standby facility. In this scenario the building is still available and the users can use normal office space to wait for systems to come on line.

Task	Team
Evaluate the damage	Disaster Management Facilities and Operations
Declare a disaster	CEO
Identify the concerned applications	IT Administrator
Request the appropriate resources at the Standby Facility	ITRT
Obtain the appropriate backups	IT Administrator
Restart the appropriate applications at the Standby Facility	IT Administrator
Inform users of the new procedures	Communications
Order replacement equipment to replace the damaged computers.	CMT and ITRT
Install replacement equipment and restart the applications	ITRT
Inform users of normal operations	Office of the CEO

**Table 4: action plan**

## 5.2 Scenario 2: major damage

In this scenario a major disaster occurred. It could be that the building communication lines are unavailable. When such major damage occurs the disaster recovery process as stipulated in the next section will be executed.

### 6 Disaster recovery processes

The LGB disaster recovery plan establishes procedures to recover LGB systems following a disruption. The plan will maximise the effectiveness of contingency operations by means of an established plan consisting of the below phases.

**Notification/activation/alert phase:** to detect and assess damage and to activate the plan

**Recovery phase:** to restore temporary business operations and recover damage done to the original systems

**Reconstitution/normalisation phase:** to restore the LGB's system processing capabilities to normal

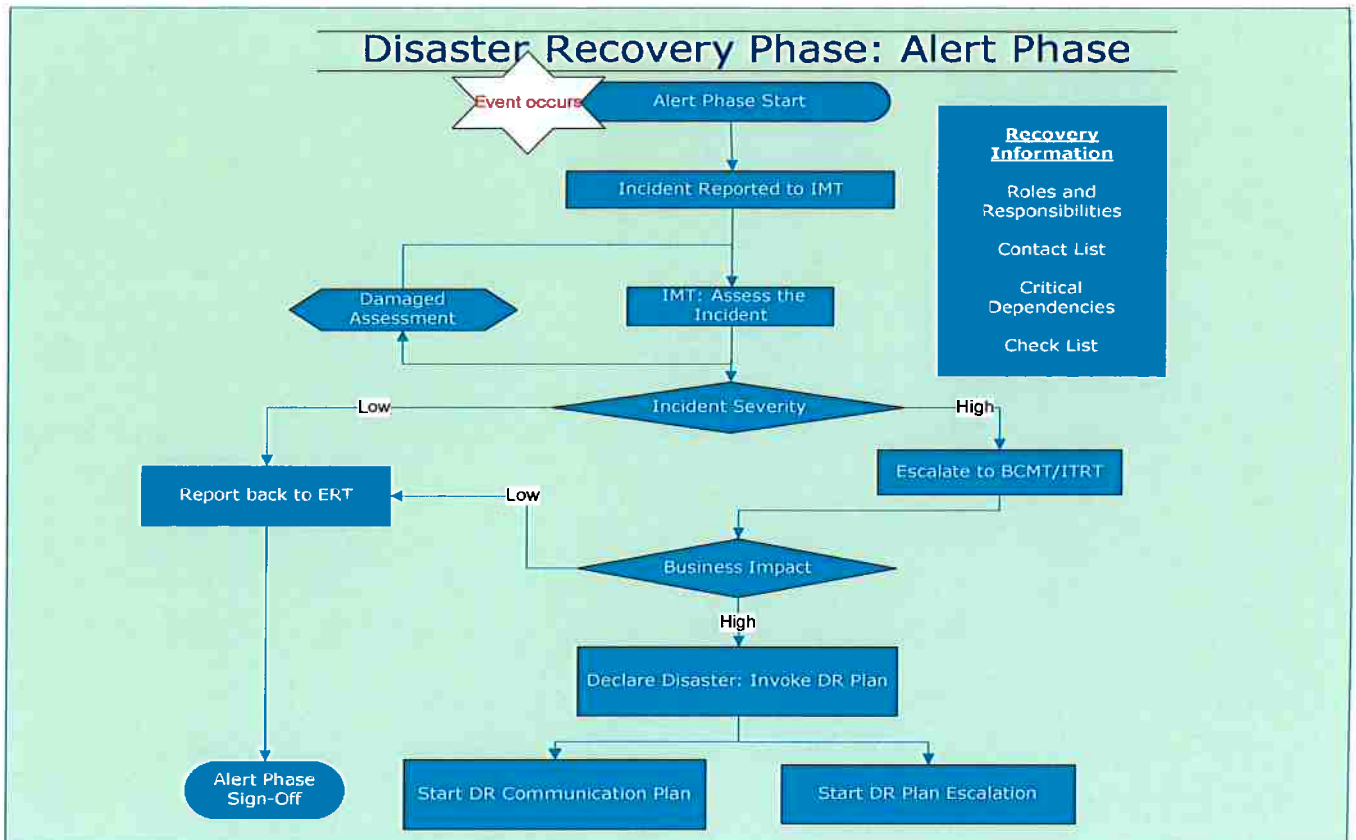
In this section the three main recovery processes, Alert, Recovery and Return to Normal, are described in detail for the Limpopo Gambling Board.

**Alert Phase:** Recovery of information

This phase deals with, and provides information that must be available prior to, and immediately after a disaster happened. It includes;

- a) reporting the incident;
- b) damage assessment procedures;
- c) escalation and declaration criteria;
- d) declaration forms to be used when declaring a disaster;
- e) internal and external communications;
- f) recovery information, including roles and responsibilities, contact detail and critical dependencies





**Figure 1: Disaster Recovery Phase: Alert Phase**

## 6.1 Reporting the incident

The person who discovers the incident must report the incident to the LGB's IT Manager at the following contact number(s):

## 6.2 Incident reporting

Support Centre	Telephone number	Alternative number
Helpdesk	015 230 2300	N/A

**Table 5: incident reporting**

The person who reports the incident must provide as much information as possible and provide the IT official with as many observations as possible. The questions that should be answered are;

- a) which applications or systems are affected?
- b) what time did the incident occur?
- c) what is the expected outage duration (if possible)?
- d) what is the damage to equipment?
- e) what is the damage to computer room environment? and
- f) any other relevant information

After the incident has been reported to the IT official should notify the incident management team of the problem. The IMT is responsible for covering the initial actions required to ensure the safety and welfare of people affected by the incident, to activate the relevant recovery management teams and determine the level of response which is appropriate to the incident.

The IMT should determine whether the nature and extent of the disruption warrant the deployment of the relevant DRP, and if so should;

- a) determine the nature of the disruption;
- b) implement the selected procedures, securing the required resources through the BCMT/ITRT where appropriate;
- c) identify, and where appropriate adapt the relevant continuity procedures to ensure that the business continues to operate as near to normal a manner as possible for the duration of the disruption. All such activities should be coordinated through the BCMT/ITRT;
- d) identify, and where appropriate adapt, the relevant recovery procedures to ensure that the business recovers from disruption in a timely and controlled manner once the root cause of the disruption has been eliminated. All such activities should be coordinated through the BCMT/ITRT;
- e) activate the BCMT/ITRT who investigates the requirement for further teams to be activated. Whilst the IMT is active, all activities should be coordinated through the BCMT/ITRT to ensure that no action taken by one IMT conflicts with actions taken by others;
- f) communicate with all parts of the Units affected by the disruption on a regular basis regarding progress and the actions initiated by the IMT;
- g) organize, once recovery actions have been completed, a thorough review of its management of the disruption so all relevant lessons from the experience can be learned and incorporated into procedures and training programmes

### 6.2.1 Assessing the incident

The LGB Disaster Recovery Coordinator, through the services of the Damage Assessment Team, will assess the damage and will evaluate the situation.

### 6.2.2 Incident management team

Members	Responsibility	Telephone number
K. Bidzha: ICT Officer	Analyse the damage at the primary site after a Disaster working together with the other members: Ensure the Integrity, Availability and Confidentiality of the damaged systems are still intact and comply to the Unit's policies. This personnel will also act as the Disaster Recovery Coordinator for IT	015 230 2323
Charles Mdluli: SCM Manager	Assist the IT manager in assessing the damage on the facility and any related peripherals	015 230 2314
Boitumenlo Mabotsa: Risk Officer	Ensure the security of the damaged environment and also security of the alternate site if relocation is required.	015 230 2313
Office of the CEO: Communications	Responsible for all communication forwarded to the Users and to the Incident Management Team	015 230 2302

**Table 6: incident management team**

### 6.2.3 Damage assessment procedures

Assets may have been damaged as a result of the disaster. The checklist below could be used to speed up the damage assessment process: Visit every instance, verify, and assess the following:

- a) IT infrastructure and services
  - i) Main computer centre
  - ii) Server room
  - iii) Power
  - iv) Air conditioning

- b) Servers
  - i) Database
  - ii) Application
  - iii) Storage
- c) Network components
  - i) Switches
  - ii) Routers
- d) Telephone systems
- e) Test main infrastructure and equipment for connectivity
- f) Record damaged equipment and infrastructure
- g) Report back to disaster recovery coordinator

### 6.2.4 Damage Assessment Checklist

Purpose:	This form is to be used to assess the damage of the systems and data within four (4) hours. It documents the assessment of the damage to the building, data center, environmental controls, and computer room contents. It provides the estimated recovery time and the equipment that may be salvaged or repaired. This form may be used to notify the IT Recovery Team of the assessment, and coordinate equipment salvage where possible. It will also be used to as input to the report to the CMT to declare the event as a disaster.
----------	--

Assess the requirement for hiring physical security to minimize possible injury, to discourage unauthorized persons from entering the facility, and to eliminate the potential for vandalism to the assets.		
Initials:	Date:	Time:

**Table 7: damaged assessment checklist**

The purpose of the checklist below is to guide a damage review and assessment of the production facilities, the network, and/or the data centre facilities following a disaster. It also documents the assessed damage for notification to the Crisis Management Team. In using the checklist, the Team must consider:

- a) The safety of the area for employees or vendors to work.
- b) The percent of normal capacity the equipment is able to function.
- c) Actions to be taken to recover or repair damaged equipment to enable functioning.
- d) Timeframes for repair or replacement of the damaged equipment to enable functioning.

Infrastructure	Damage		Salvageable		Description of damage
	YES	NO	YES	NO	
<b>Building</b>					
Exterior	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Interior	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>Data Centre</b>					
Walls	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Ceilings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Floor	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>Environmental controls</b>					
Electrical	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Infrastructure	Damage		Salvageable		Description of damage
	YES	NO	YES	NO	
Air-con	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Water supply	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Fire suppression	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>Computer Room</b>					
Servers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
External Disk Drives	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Tape Backups	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Network Cabling	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Communications	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Terminals	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Equipment	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Magnetic Tape Media	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Spare Parts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>Office content</b>					
Workstations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

**Table 8: description of damage checklist**

Estimated Recovery Time		
Based upon the damage assessment, determine the estimated recovery time based upon the following guidelines		
<input type="checkbox"/>	Non-Disaster: Minimal damage to the facility and/or equipment. Estimated time to complete repairs is less than 24 hours.	
<input type="checkbox"/>	Minor Disaster: Moderate damage to the facility and/or equipment. Estimated time to complete repairs is between 24 hours to 7 business days	
<input type="checkbox"/>	Catastrophic Disaster: Extensive damage to the facility and/or equipment. Estimated time to complete repairs is greater than 7 business days.	
Initials:	Date:	Time:

**Table 9: estimated recovery time checklist**

Salvage and repair					
Identify equipment, documentation, or spare parts that are immediately salvageable or needing repair.					
Item	Salvage	Repair	Location	Sent to	Date
	<input type="checkbox"/>	<input type="checkbox"/>			
	<input type="checkbox"/>	<input type="checkbox"/>			
	<input type="checkbox"/>	<input type="checkbox"/>			
	<input type="checkbox"/>	<input type="checkbox"/>			
Initials:	Date:		Time:		

**Table 10: salvage and repair checklist**

<b>Verbal notification</b>		
Verbally notify the Management Team of the conducted survey, damage assessment, estimated recovery time and damaged and potentially salvageable equipment.		
Initials:	Date:	Time:

**Table 11: verbal notification checklist**

<b>Recovery briefing</b>	
Attend the recovery briefing scheduled by the IT Operations Recovery Management Team to apprise Recovery Teams members of findings.	
<b>Date / time of meeting:</b>	<b>Subject of meeting :</b>

**Table 12: recovery briefing checklist**

<b>Equipment movement</b>			
If emergency mode operations will take place at a recovery site, the following, salvageable equipment should be transported to the alternative site.			
<b>Equipment</b>	<b>Description</b>	<b>Contractor to move equipment</b>	<b>Date of move</b>
Initials:		Date:	Time:

**Table 13: equipment movement checklist**

The team should coordinate with the Management Team, vendors, and suppliers to restore or repair salvageable equipment. It should assist in the clean up of the disaster area to permit eventual renovation and/or reconstruction. Under no circumstances should the Damage Assessment and Salvage Team make any public statements regarding the disaster, its cause, or its effects on the organisation's operations.

The team shall not enter a disaster area until emergency personnel give permission.

### **6.2.5 Escalation**

Once the failure or disruption has been properly assessed, and established that it has an impacts on the maximum allowable downtime window, thereby posing a possible business risk; Crisis Management Team needs to be notified of the situation and the members are as follows is as follows:

### **6.2.6 Crisis Management Team**

<b>Designation</b>	<b>Name</b>	<b>Contact no.</b>	<b>Alternative no</b>

CEO		015 230 2302	0828082488
CFO	M. Mathabatha	015 230 2306	082 578 5978
ICT	M. Lavhengwa	015 230 2322	082904 4201
HR Manager	E. Makgoba	015 230 2319	082 837 1018

**Table 14: crisis management**

The Crisis Management Responsibilities are as follows:

- a) manage communication with regulators, investors, the media, associates and staff;

The Crisis Management team should engage other Business Units Managers to assess the impact of the incident and the downtime. A list of these managers is attached, see Annexure B.

Should business units managers decide that the incident has no immediate impact on the business, the Help Desk will be notified and the incident will be closed, or depending on the situation, be resolved as a fault.

Should Business Unit Managers however decide that the incident impacts negatively on the maximum allowable downtime window, a disaster is declared. The CMT informs the IMT which informs the BCM/ITR Team and the BCM/ITR Team invokes the DR plan.

### 6.2.7 Disaster Declaration Authority

Making a wrong decision to declare a disaster could be a costly exercise. The correct level of authority should therefore be defined. In the event of a disaster, only the people listed below is empowered to declare and invoke a disaster:

### 6.2.8 Designated authorities who may declare a disaster

Designation	Name	Contact no.	Alternative no
CEO	Serobi Maja	015 230 2302	082 808 2488
CFO	M. Mathabatha	015 230 2306	082 578 5978
ICT Officer	K. Bidzha	015 230 2323	082 333 8084

**Table 15: designated authorities**

### 6.2.9 BCMT/ITRT team

Members	Responsibility	Telephone number	Alternative number
IT Officer : K. Bidzha	Project Management and overseeing that the recovery process is properly resourced. Organize all required recovery Teams.	015 230 2323	082 333 8084
DR Coordinator: K. Bidzha	Coordinate the implementation of DRP if the disaster strikes	015 230 2323	082 333 8084
Network Specialist: K. Bidzha	Recovery of the communication networks	015 230 2323	082 333 8084
Communication: CEO's office	Responsible for all communication that is sent to the Incident Management Team	015	
Database Administrator: K. Bidzha	Recovery of systems Databases	015 230 2323	082 333 8084
Backup Administrator: K. Bidzha	Fetch required tapes and restore of all backups and backup of both the Primary and alternate site data.	015 230 2323	082 333 8084

**Table 16: BCMT/ITRT Teams**

The BCMT/ITRT is responsible for:

- a) ensuring that all the facilities, people and other resources that they require to mount effective response, continuity and recovery operations;
- b) coordinate the allocation of resources
- c) manage communication with IMT;
- d) DR Briefing

### 6.3 Recovery phase

This phase deals with, and provides information that will be required to restore the system to a state of normality after a disaster has struck. It includes:

- a) DR briefing and analysis of damages from the assessment
- b) Backup procedures
- c) Recovery procedures

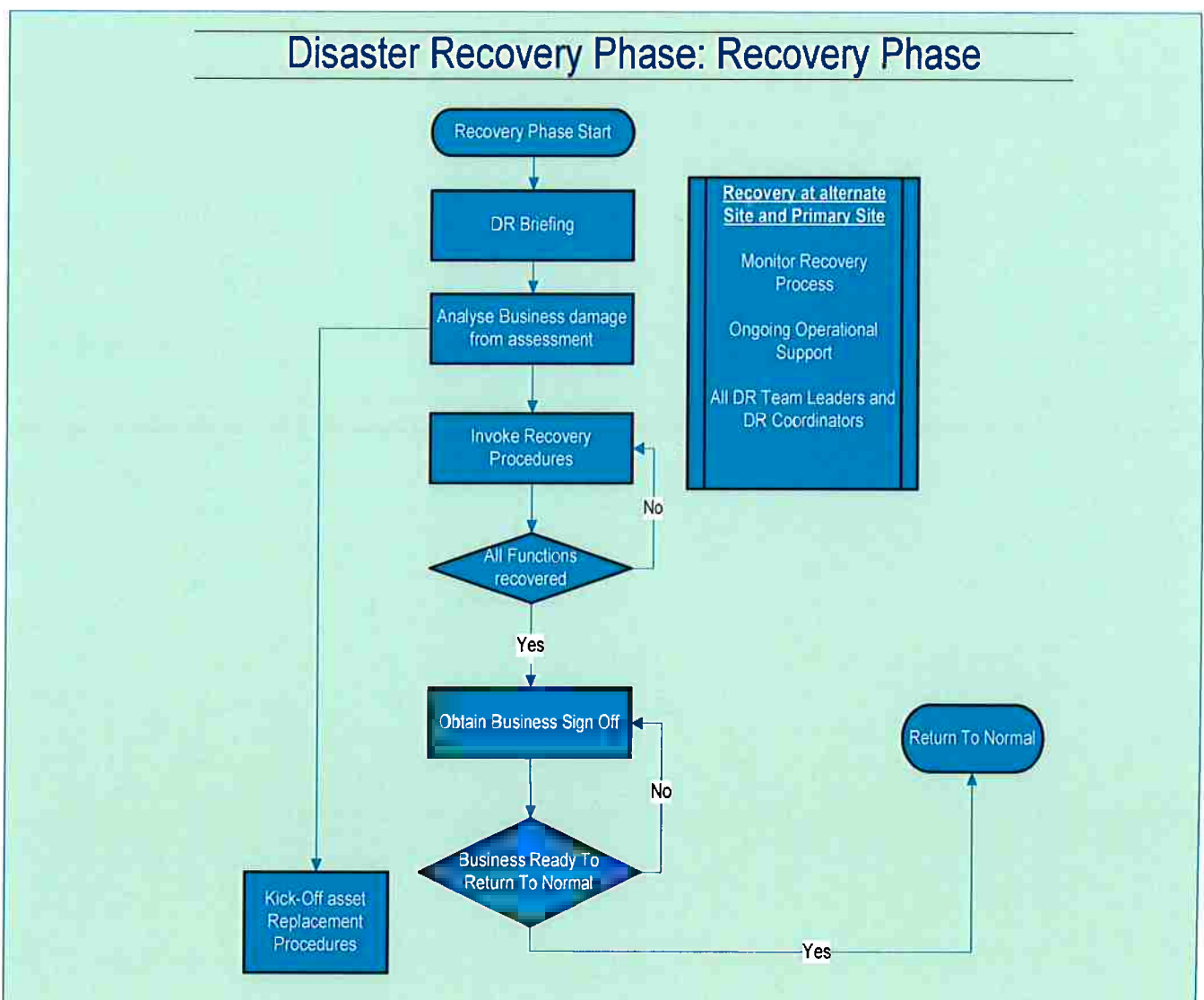


Figure 2: Disaster Recovery Phase: Recovery Phase

### 6.3.1 DR briefing and analysis of the damage assessment

The recovery process starts with an information session with all relevant recovery teams. The issues addresses during that meeting are;

- a) the recovery phase is officially activated;
- b) the damage assessment report is analyzed;
- c) the recovery team members review the status of their respective areas of responsibility;
- d) the DR Coordinator reviews the overall plan with the team members;
- e) any adjustments to the Disaster Recovery Plan to accommodate special circumstances are decided upon; and
- f) ongoing meetings for the duration of the recovery phase are scheduled

### 6.3.2 Invoke recovery procedures

#### 6.3.2.1 Backup procedures

The following roles and responsibilities will apply for this policy and procedures:

### 6.3.3 Backup personnel contact details

Name	Designation	Work Tel	Cell #
K. Bidzha	Backup Administrator	015 230 2323	082 333 8084
K. Bidzha	Offsite Backup Personnel	015 230 2323	082 333 8084

Table 17: backup personal contact details

#### 6.3.3.1 Request and delivery of required backup tapes

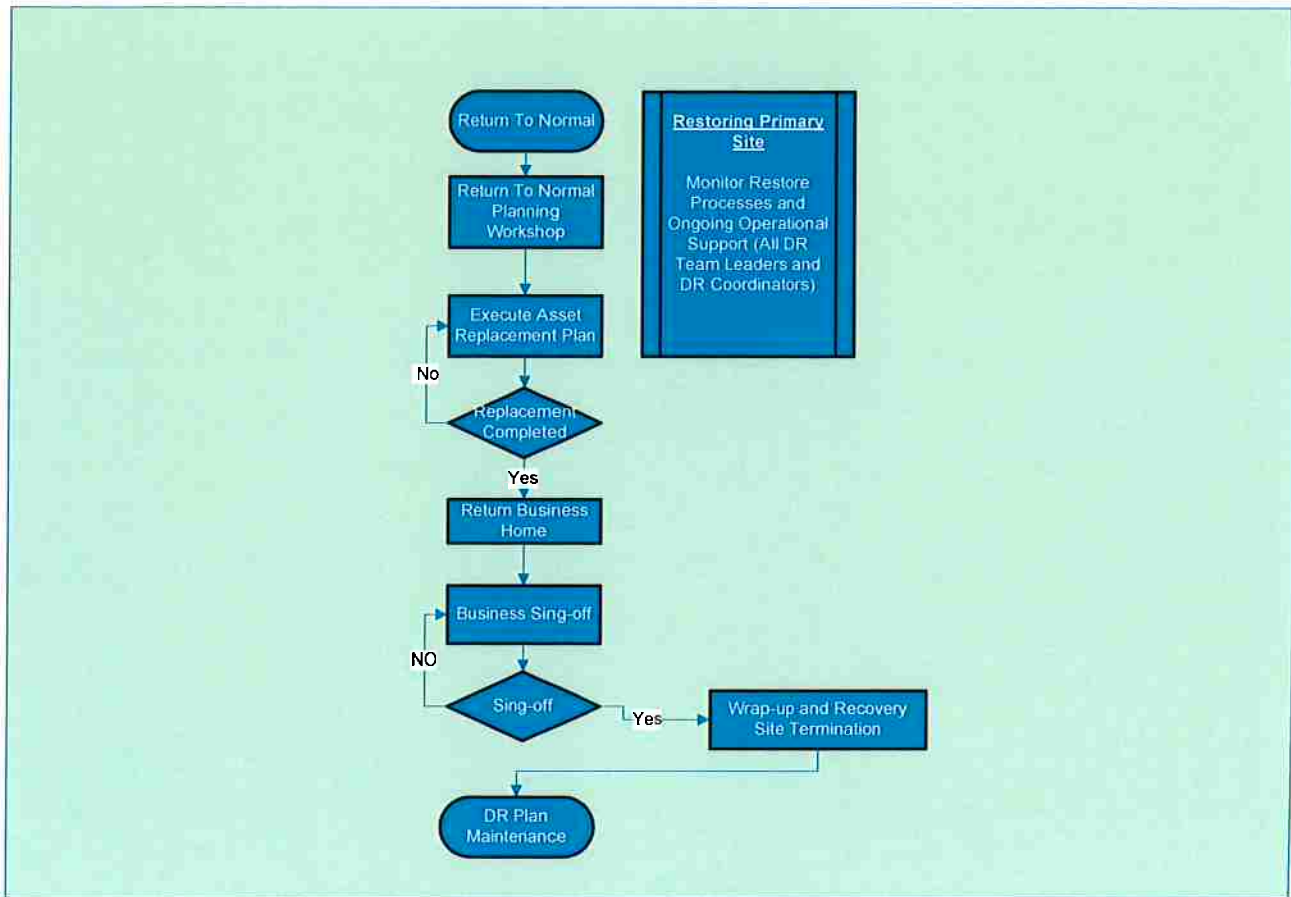
Backup Administrator needs to collect the required backup tapes. The off-site personnel on the off-site storage side will identify the correct full backup tape as well as the incremental backup tape. The Backup Administrator is requested as a matter of urgency to transport the tape from off-site storage centre to DR Site data centre. The backup site will be standard back square corner Thabo Mbeki and Hans Van Resenberg at Standard bank in Schoeman Street Polokwane. Limpopo Gambling Board will also use **own cloud** as a backup mechanism for the identified system and records.

### 6.4 Return to normal phase

This phase deals with, and provides;

- a) information that will be required for the replacement of damaged assets which may have resulted from the disaster;
- b) the transfer of recovered systems from the standby recovery facility to the home site computer centre; and
- c) maintenance and testing of the plan





**Figure 3: Disaster Recovery Phase: Return to normal Phase**

## 6.4.1 Information requirements

### 6.4.1.1 Return to normal checklist

Once the building and associated infrastructure are restored at the primary datacenter (on original or new site) and staff are ready, then a planned transfer of the workload from backup site to primary site can begin. This is essentially a reversal of the procedures by which transfer to the DR site was attained.

These steps will take the form:

Steps	YES	Remarks
Confirm primary site operational	<input type="checkbox"/>	
Confirm the integrity of Primary site systems	<input type="checkbox"/>	
Backup site will be informed and begin local preparations for transfer of data	<input type="checkbox"/>	
Transfer of staff from Backup site	<input type="checkbox"/>	
Make any local configuration changes required to accommodate third party connectivity	<input type="checkbox"/>	
Ensure connectivity to Primary system	<input type="checkbox"/>	
Individual site managers will be informed	<input type="checkbox"/>	
Help Desk will be formally informed that the primary site is operational again	<input type="checkbox"/>	
Other third parties will be informed (e.g. IT Master)	<input type="checkbox"/>	
The Disaster Recovery Plan will be reviewed in conjunction with the Disaster Recovery Coordinator and updated with any lessons learned from the live Disaster Recovery	<input type="checkbox"/>	
Communicate changes to all interested parties,	<input type="checkbox"/>	

Steps	YES	Remarks
including third parties		
The disaster recovery team will be de-briefed and disbanded	<input type="checkbox"/>	

## 6.5 Damage assessment and salvage team

The ITR Team is responsible for the assessing the damage to the LAN and LAN facilities and reporting the level of damage to the Incident Management Team. They must perform the assessment as quickly as possible following the disaster. The team is also responsible for overseeing the salvage operations required to clean up and repair the data center and for re-establishing the data center in the reconstituted or new site.

### 6.5.1 Damage assessment and salvage team responsibilities

Post-disaster responsibilities	
<input type="checkbox"/>	Determine damage and accessibility to: <ul style="list-style-type: none"> <li><input type="checkbox"/> The building,</li> <li><input type="checkbox"/> The data centre,</li> <li><input type="checkbox"/> The LGB's offices,</li> <li><input type="checkbox"/> Environmental controls,</li> <li><input type="checkbox"/> Computer room contents, and</li> <li><input type="checkbox"/> Office contents. (From the Damage Assessment Checklist)</li> </ul>
<input type="checkbox"/>	Assess the extent of damage to the LGB's LAN and data center.
<input type="checkbox"/>	Assess the need for physical security. (e.g., security guards)
<input type="checkbox"/>	Estimate recovery time based upon the damage assessment. (From the Damage Assessment Checklist)
<input type="checkbox"/>	Identify salvageable hardware and communication equipment.
<input type="checkbox"/>	Apprise the Management Team on the extent of damages, estimated recovery time, required physical security, and salvageable or repairable equipment.
<input type="checkbox"/>	Maintain salvageable hardware and equipment log.
<input type="checkbox"/>	Coordinate with vendors and suppliers in restoring, repairing, or replacing salvageable hardware and equipment.
<input type="checkbox"/>	Coordinate transportation of salvaged equipment to recovery site, if necessary.
<input type="checkbox"/>	Provide support in cleaning up the data center following the disaster.

**Table 18: damaged assessment and salvage team responsibility**

## 6.6 Physical security team

The Physical Security Team provides personnel identification and access limitations to the building and floors and acts as a liaison to emergency personnel. This is crucial during the time of a disaster because of the uncommonly large number of vendors, contractors, and other visitors requiring access to the building and floors.

### 6.6.1 Physical security team responsibilities

Post-disaster responsibilities	
<input type="checkbox"/>	Assess damage to entries to the disaster site.
<input type="checkbox"/>	Act as a liaison to emergency personnel, such as fire and police departments.
<input type="checkbox"/>	Cordon off the data center to restrict unauthorized access.
<input type="checkbox"/>	Coordinate with Facility or Building Management for authorized personnel access.
<input type="checkbox"/>	Provide security guards, as required.
<input type="checkbox"/>	Schedule security for transportation of files, reports, and equipment.
<input type="checkbox"/>	Provide assistance in any official or insurance investigation of the damaged site.

**Table 19: IT physical security team responsibility**

### 6.6.2 Communications team responsibilities

Post-disaster responsibilities	
<input type="checkbox"/>	Coordinate with the ITR Team on assessing communications equipment needs
<input type="checkbox"/>	Coordinate with the IT Technical to determine communication and network equipment needs.
<input type="checkbox"/>	Coordinate with LGB Management Team to procure needed communication equipment.
<input type="checkbox"/>	Coordinate with LGB Management Team to procure needed cabling.
<input type="checkbox"/>	Retrieve the communications configuration from the off-site storage unit.
<input type="checkbox"/>	Plan, coordinate, and install communication equipment at the alternative site.
<input type="checkbox"/>	Plan, coordinate, and install network cabling at the alternative site.

**Table 20: IT communication team responsibility**

### 6.6.3 Hardware installation team responsibilities

Post-disaster responsibilities	
<input type="checkbox"/>	Verify the pending occupancy requirements with the alternative site.
<input type="checkbox"/>	Inspect the alternative site for physical space requirements.
<input type="checkbox"/>	Notify the recovery site of impending occupancy.
<input type="checkbox"/>	Interface with the IT Technical about the space configuration of the alternative site.
<input type="checkbox"/>	Coordinate the transportation of salvageable equipment to the alternative site.
<input type="checkbox"/>	Plan the hardware installation at the alternative site.
<input type="checkbox"/>	Install hardware at the alternative site.
<input type="checkbox"/>	Plan, transport, and install hardware at the permanent site, when available.
<input type="checkbox"/>	Set up and operate a sign-in, sign-out procedure for all equipment sent to and from the alternative site.

**Table 21: hardware installation team responsibility**

### 6.6.4 IT recovery team responsibilities

Post-disaster responsibilities	
<input type="checkbox"/>	Assist the IT Technical Team as required.
<input type="checkbox"/>	Schedule a new pickup location with the off-site storage unit.
<input type="checkbox"/>	Arrange for the delivery of off-site storage containers.
<input type="checkbox"/>	Receive the delivery of off-site storage containers.
<input type="checkbox"/>	Ensure backup tapes are sent to the off-site facility for storage.
<input type="checkbox"/>	Return backup medium in storage containers to the off-site storage unit.
<input type="checkbox"/>	Set up and operate a sign-in, sign-out procedure for all IT materials sent to and from the alternative site.
<input type="checkbox"/>	Check the alternative site's floor configuration to assist the Hardware, Software, and Communications Teams with installation plans.
<input type="checkbox"/>	Monitor the security of the alternative site and the LAN network.
<input type="checkbox"/>	Coordinate the transfer of equipment, furniture, and personnel to the alternative site.

**Table 22: IT recovery team responsibility**

### 6.6.5 IT technical team responsibilities

Post-disaster responsibilities	
<input type="checkbox"/>	Restore operating systems, applications, and network software from backup medium.
<input type="checkbox"/>	Initialise new tapes as needed in the recovery process.
<input type="checkbox"/>	Conduct backups at the off-site location.
<input type="checkbox"/>	Test and verify operating systems, applications, and network software.
<input type="checkbox"/>	Modify the LAN configuration to meet the alternative site configuration.

**Table 23: IT technical team responsibility**

### 6.6.6 Asset replacement procedures

The following checklist should be used to speed up the asset replacement process:

- a) get detailed information on impact of disaster;
- b) determine specifications of hardware required based on the relevant asset register
- c) determine versions and specifications of software required based on the information provided by relevant role player;
- d) determine supplier that will respond fastest;
- e) get delivery date from supplier;
- f) get estimated costs for replacement;
- g) complete the asset purchase documentation; and
- h) get management approval of the order

In the case where an asset is damaged the following RACI needs to be populated. This will identify time delays when replacing hardware and/or software and identify time impact on RTO.

### 6.6.7 Damage assessment checklist

Impacted Asset	Impact Description	Hardware /software Specifications	Time of impact	Approving manager	Delivery date	Time after asset fixed	Time elapsed

Table 24: damaged assessment checklist

### 6.6.8 Disaster recovery plan maintenance

#### 6.6.8.1 Plan maintenance checklist

The following list should be used as a guideline/reminder to maintain important elements of the Plan. As a minimum requirement, the Plan should be validated every 12 months.

Plan Element	Responsible Person/Team	Plan validation completed (y/n)
Maintaining the strategy, plans and procedures	DR Coordinator	ITR Team
Ensuring education and awareness of disaster recovery is given sufficient prominence	DR Coordinator	ITR Team
Review of the Plan and risks (with their associated reduction measures), testing of the Plans, controlling changes to the strategy and the Plans so these are maintained to be consistent with each other	DR Coordinator	ITR Team
Training people to produce the strategy and Plans as well as to undertake the actions embodied within the Plans	DR Coordinator	ITR Team
Assurance of the quality and applicability of the plans. In this context quality refers to adaptability, completeness, data quality, efficiency, friendliness/usability, maintainability, portability, reliability, resilience, security, testability and timeliness	DR Coordinator	ITR Team

Table 25: planned maintenance checklist

### 6.6.8.2 Plan maintenance schedule

The DRP must be kept up to date to reflect changes in the business. The following schedule should be adhered to:

Type of change that will influence the contents of the Plan	Responsible Person/Team	Plan update completed (y/n)
Additions, deletions, or upgrades to hardware platforms.	DR Coordinator and Technical Administrator	
Additions, deletions, or upgrades to system software.	DR Coordinator and Technical Administrator	
Changes to system configuration	DR Coordinator and Technical Administrator	
Changes to applications software affected by the Plan	DR Coordinator and Technical Administrator	
Changes that affects the availability of the Alternative DR facility	DR Coordinator and Technical Administrator	
Changes to contact lists (including vendors/suppliers)	All parties involved	

Table 26: type of change

### 6.6.9 Disaster recovery plan testing

Individual elements of each DRP need to be tested (or practiced or rehearsed). Final sign-off of a particular Plan or element of a Plan depends on when testing can be carried out. Guidelines on testing of the Plan include:

- a) Testing of the Plan could be in the form of a 'desk check' or detailed technical testing.
- b) An initial technical test can usually be done without the need to involve the business, such as acceptance of a new IT system. However, for subsequent tests it is prudent to get the business to be involved to 'prove' the capability and to aid mutual understanding of the activities and resources needed to achieve the common goal of business recovery.
- c) Tests may be announced or unannounced; however, in the latter case it is necessary to ensure that senior Management approval is obtained in advance otherwise it may be difficult to achieve commitment.

#### 6.6.9.1 Issues to consider when planning for a test

Tests are likely to disrupt the business. When testing DRPs, it is prudent to consider:

Issues	Comments
Is it possible to time this testing to cause least disruption to your business functions or less upset to your customer?	
How much will the test cost? – is this appropriate for the additional confidence gained over other forms of testing, including a desk check?	
How can staff be trained to cope with the situation if they do not experience it in rehearsal-mode?	
Once the DRP is in operation – how will you return to normal business operations? – are there specific issues here that warrant testing in their own right?	

Table 27: issues to consider during testing

### **6.6.9.2 Limpopo Gambling Board's testing procedures**

Customer logs a call at helpdesk and requests to "initiate the disaster recovery plan".

(Note: Pls confirm that the call is routed to ITR Team)

Helpdesk logs call and immediately notifies the operations team and supply the request reference number.

ITR team assesses the situation and determines whether they are able to recover system within one hour of the call being logged or a problem being detected. (In a test situation the answer is NO).

ITR team will invoke disaster recovery plan on their system and follow the instructions.

The test coordinator should;

- a) note whether the operations officer uses the "quick guideline" option to get acquainted to the system (please explain this!);
- b) refer to the strategy option to get an idea of the process;
- c) start recovery by beginning at the top of the flowchart;
- d) notify the relevant staff as specified;
- e) note any changes necessary to recover effectively; and
- f) record time it takes to recover system from the moment the call was logged

Once the system is working in backup mode users must ensure integrity and availability of data.

Once they are satisfied, they should contact the IRT team staff to notify that they are satisfied with the test.

ITR Team staff must then initiate the normalization process and verify that all system is available.

DR Coordinator to setup post test meeting to discuss any issues that need attention. All parties who were involved in the pre-test meeting need to identify all the issues, which came up during the test, and such issues need to be resolved as a matter of urgency.

## **Annex A. Acronyms**

---

BCI	Business Continuity Institute
BCP	Business continuity plan
COBIT	Control Objectives for Information Technology
CCTV	Closed circuit television
DRP	Disaster recovery plan
DRII	Disaster Recovery Institute International
HVAC	Heat ventilation and air conditioning
ISF	Identity security forum
ISS	Information system security
ISO	International Standards Organisation
IT	Information Technology
ICT	Information and Communication Technology
ID	Identity document
LOB	Line of business
PFMA	Public Finance Management Act
R	Rand
SMS	Short message services
UPS	Uninterruptable power supply