IT Disaster Recovery Plan Template

 Document Control

|  |  |
| --- | --- |
| Author | Mary Mbugua |
| Document Reference | SIL-TPL-009\_v1.0 |
| Document Version | 1.0 |
| Date | 04/02/202016/06/20 |
| Distribution | Silensec |

**CONFIDENTIALITY**

The content of this document is CONFIDENTIAL and property of Silensec. It contains confidential information that captures Silensec know how and expert knowledge. Any reproduction and/or circulation, either electronic or by any other means is forbidden without prior approval by Silensec. Circulation is STRICTLY limited to the stated recipients.

**Copyright © 2020 Silensec Limited. All Rights Reserved**

Table of Contents

1. SCOPE 3

2. RECOVERY OBJECTIVES 3

RECOVERY TIME OBJECTIVE (RTO) 3

RECOVERY POINT OBJECTIVE (RPO) 3

3. RECOVERY team 4

A. SERVICE / ROLE / FUNCTION 4

B. RESPONSIBILITY 5

C. DEPENDENCIES 6

D. EXPECTED RESPONSE TIME 9

4. RECOVERY STRATEGY 9

A. INITIAL RECOVERY 9

B. OVERALL RECOVERY STRATEGY 9

**RECOVERY SCENARIOS** 10

5. RETURN TO OPERATIONS 10

# SCOPE

Service Area, Service Offerings, Service Areas that depend on the service at risk

|  |
| --- |
| A disaster recovery plan (DRP) is a documented, structured approach that describes how Botswana Examinations Council (BEC) can quickly resume work after an unplanned incident. A DRP is an essential part of a business continuity plan (BCP) and applied to the aspects of BEC that depend on a functioning IT infrastructure services. These DRP aims to help BEC to resolve data loss and recover system functionality so that it can perform in the aftermath of an incident, even if it operates at a minimal level. Some of the core IT functions that is covered by DRP includes but not limited to are; BEC core Examinations processing system (Malepa), accounting and financial systems (Accpac), Data file server as well as Core ICT Infrastructure services like networks, domain servers and backup data recovery processes. The step by step procedure of BEC ICT infrastructure restore and recovery procedure is covered on these DRP as well as ICT recovery team. The restore and recovery standards are also defined |

# RECOVERY OBJECTIVES

## RECOVERY TIME OBJECTIVE (RTO)

The maximum length of time IT processes can be down before the disruption impacts the business

|  |
| --- |
| The amount of time between the disasters and when services are restored are factored by disaster recovery (DR) site of BEC. BEC has site aside a DR site with up and running infrastructure equipment (such as workstations, servers, storage) and networking infrastructure in which cores business applications of BEC can be restored and recovered as well as contractual vendors. The RTO parameter for BEC is quantified as follows in case of disaster;* Replicated servers, Applications and Data – 2Hours
* Malepa restore and recovery from backups tapes to DR servers – 6hours

Therefore RTO for critical mission business systems like Malepa is 8Hours  |

## RECOVERY POINT OBJECTIVE (RPO)

The maximum interval of data loss since the last IT service backup that the business can tolerate while still proceeding with normal business processes

|  |
| --- |
| In order to minimise data loss, BEC ICT team has set a schedule to perform incremental backup of critical business data and mission critical production Databases like Malepa twice in a day. The first backup scheduled at 12 noon and the last scheduled at 1800hrs during the day. Therefore the allowable data loss critical system is **4 hours** |

# RECOVERY team

## SERVICE / ROLE / FUNCTION

|  |
| --- |
| A disaster recovery team is a group of individuals from BEC staff who are tasked with developing, documenting, and executing processes and procedures for BEC data recovery, business continuity, and IT infrastructure in the event of a disaster or failure. The disaster recovery team includes the following roles and functions;* **BEC Executive management**

The Executive management team are not heavily involved in IT disaster recovery planning, but plays pivotal oversight role for strategy, policy and budgetary approvals.* **ICT Head of Recovery team**

 The head of DR team is BEC ICT director, as an executive management team member. Their job is to supervise the entire team, coordinate the efforts of each member and ensure an efficient DR plan is in place.* **Impact assessment, Restore and Recovery team**

The impact assessment, restore and recovery team is the most responsible for the actual IT and data recovery event. The restore and recovery team for BEC is made of ICT Operations manager, ICT Operations coordinator, ICT Infrastructure-Servers, ICT Infrastructure-Networks who are mostly experts of servers, Networks, storage and Databases. The team is accountable for identifying, implementing and testing the correct solutions and strategies that will ultimately recover business operations. These strategies should be focused on meeting the demands of the critical business units identified within the BIA.* **ICT Applications Support**

The ICT Applications support have a varying level of influence and responsibility depending on the recovery plan and the amount of data loss as well as the severity of the disruption caused. The application support would know exactly which application tasks need to be executed based on the restoration plan, including:* **Business continuity expert –Compliance and Quality Assurance(CQA)**

Business continuity is an integral part of disaster recovery plan hence BEC need to include CQA as part of recovery team. Business continuity sets out the groundwork and strategy needed to allow business to continue operations as well as standards and procedure compliance for a recovery operations. CQA may considers the whole of the organization but in ICT disaster recovery planning, it focuses on processes, standards and procedures for specific technologies and business functions during recovery instance. |

## RESPONSIBILITY

|  |
| --- |
| Each members of BEC ICT Disaster recovery team has some clear responsibilities as follows;* **BEC Executive management**

The Executive management team are responsible for oversight of strategy, policy and budgetary approvals for DRP.* **Business continuity expert –CQA**

CQA as business continuity expert have two responsibilities in BEC ICT disaster recoveryplan:* + Make sure that the DR strategy and plan is in alignment with business needs, which have been determined by a thorough Business Impact Analysis (BIA). The BIA should be complete before DR planning starts. The proper analysis identifies specific goals and allows DR efforts to support actual recovery needs.

To keep everyone on the same page, the business continuity expert should facilitate open communication between business and ICT, making sure they are together in purpose and alignment.* + Confirm that the critical pieces of the business continuity plan are also present in the DR plan. The ICT team has the technology know-how, but they might not be aware of some business fundamentals that play a role in an emergency: correct reporting procedure in the midst of an event, contact information for critical personnel and vendors, etc.
* **ICT Head of Recovery team**

 BEC ICT director is responsible for development of DRP and makes sure that processes, standards and procedures are developed for DRP.* **BEC Critical business unit advisors – Office of Strategy (OSM)**

Office of strategy management may not directly involved in the DRP executions but has great responsibility to represent business unit within the BIA to provide feedback on DR planning efforts. * + OSM proactive provide input from unit advisors while the plan is in the initiation stage. This helps identify which business processes will be affected by proposed BEC ICT recovery steps, and provides the opportunity to discuss feasibility.
	+ They advises on the risk of recovery efforts that will negatively affect the needs of a business unit.
* **Impact assessment, Restore and Recovery team**

The impact assessment, restore and recovery team is made of three roles (ICT Operations manager/coordinator, Infrastructure Analyst-Servers, Infrastructure Analyst-Networks) with their specialised responsibility in DRP team as follows;* **ICT Operations manager/Coordinator**

The ICT Operations manager/Coordinator is responsible for supervising and coordinating the DR implementation team member. Their role is to supervise the entire team, coordinate the efforts of each member and ensure an efficient DR plan is in place and implementable (BEC data backups are performed). The role has the responsibility of assessing the impact analysis of disaster to BEC business functions in lieu with infrastructure analyst team* **Infrastructure Analyst-Networks (IAN):**

 The Infrastructure Analyst-Networks plays key responsibility during disaster recovery and pre disaster incident by making sure that BEC ICT Networks are recoverable during disaster and become available for business functions. The role ensures BEC network infrastructure and TELECOM infrastructure like IP phone connectivity are recoverable during DR event. These role ensures replications of core business application servers across to DR site and backups of business data on daily bases on external medias like tapes and Network Attached Storage (NAS). It is also the responsibility of IAN to ensure that network connectivity are restored back after disruption to both internal and external customers. * **Infrastructure Analyst-Servers (IAS):**

The IAS works hand in hand with IAN to recover servers back to their normal operations after disaster disruptions. These two roles expertise on servers and operating systems infrastructure utilised by BEC. The IAS role is responsible for implementing data recovery backups on the chosen replication technologies and backup software tools – Oracle Secure backups and HP VM explorer. **Storage: -** Storage is one of the key responsibility of IAS during DR event. IAS ensure accessibility of data recovery at storage level is available for servers and servers rely on the underlying data storage to provide business functions services. SAN storage are at the centre of your recovery capability and strategy. **Database administration:** - it is the responsibility of IAS as member of DR team to restore and recover databases from backup medias for all mission critical BEC business systems during DR incident. IAS knows all data disk and operating system disks which are required for servers and data recovery to bring up functional business systems.* **ICT Applications Support**

The ICT applications monitor knows exactly which application tasks need to be executed based on the restoration plan and some of his responsibility in the DR team includes:* + **Data consistence** – During disaster recover executions, some application data may be inconsistent and requires application support specialist to run consistence checks
	+ **Application integrations** – App integrations may be affected and requires application support to re-integrate the applications.
	+ **App settings and configuration** – Reconfigurations of application to point to the correct servers may be required after recovery and some setting may have changed which requires changes on the application settings.
 |

## DEPENDENCIES

|  |
| --- |
| BEC ICT DRP depends on the availabilities of the following ICT infrastructural tiers and recovery procedures which will easy the executions of the DRP;* **Key Critical Business Processes systems**

BEC ICT DRP depends on the availability of the key business processes and the recovery team will depend on those identified process which are prioritised first for recovery. Some of the key business process include;* + Examination Processing - Malepa
	+ Procurement and vendor payments processing - ACCPAC
	+ HR and Payroll processing – VIP/ESS

These processes are prioritised according to their criticality of the business requirement and DRP team will depends on the impact analysis of these processes (BIA).  * Tier 1:- **Data Backup with No Hot Site**

Business Tier 1 continuity solutions are those that make backups at specific time intervals, and then physically ship those backups off-site for storage. BEC ICT backup its data to external medias like TAPES and external disks – Network attached storage (NAS) for offsite shipping. The tapes are taken to contracted company called Document bank and collected on monthly bases. However, DRP team depends on the availability of these offsite Tapes as well as functional backup software. BEC uses three software for backups; Oracle Secure Backup (OSB), HP VM explorer and Symantec Backup Exec. The recovery team depends on the proper functioning of these three applications to meet BEC RTO and RPO. During DRP executions, the team request for delivery of those Tapes from offsite storage and insert into media library at DR site for data restores and recovery. To avoid the risk of data or tapes loss, tapes are locked into cases accessible only to the authorised individuals from BEC ICT Recovery team. The keys are only accessible to that team member only. The tapes are also physically locked to minimise the risk of information reading and leaking. To avoid the risk of losing of all recovery hardware, media tape library is kept at DR site and Databases backups are pushed across the network to DR site. The data are encoded such that data loss or packet sniffing is protected during data transit.* **Tier 2:- Data Backup with a Hot Site/DR site**

Tier2 has similarities with disaster recovery at Tier 1 and it provides a backup computer system (hot site) at a remote physical location. BEC has set aside DR site at PPADB and provides similar ICT infrastructure though less processing power for fail over and disaster recovery purpose. HP VM explorer software is used to copy and backup critical server images at DR site through snapshot technology. The restore and recovery team operationalises these online backups and a schedule has been configured on HP VM explorer to run automatically on certain intervals. These DR systems is capable of handling the same data processes as the primary system. If a disaster event occurs, the backups can be restored on this backup system. The DRP execution therefore deeply relies on the availability and the functionality of DR site and proper configurations of HP VM explorer software. This approach allows faster system restoration as only the data, and not the system itself, has to be restored. Furthermore to minimise data loss, BEC DRP requires additional license for Oracle data guard to perform hot site replications of the core Examinations processing system (Malepa) that would reduce down time to zero and recovery team will take some few minutes to switch over and failover to DR site in case of catastrophic incident. DRP explicitly depends on the availability of the data guard licence to maintain RTO lower and no need to start restore and recovery processes but rather switchover and failover is performed on DR site and make it production site. The remote site will be able to start working in less time, thus significantly reducing RTO.**Tier 4: Point-in-Time Copies**BEC ICT has adopted Tier 4 as a mechanism to speedup data backup and recovery by backing some of its daily, weekly and monthly backups on Network attached storage (NAS) devices. The NAS backup employs faster storage mediums for backups on the hard drives instead of tapes. The drives have faster access times, but still need to be shipped to a remote storage location across the BEC ICT network. The DR team depends on the availability and data restore and recovery speed of reading data from backup drives. These tier make use of compressions to increase the speed of writing data to the backup drives and, even more importantly, speeds up recovery. Recovering from disk can be done at granular level (File level) and DR team can recover the BEC data at file level hence lower chance of data loss.**Tier 5: Backup Data Integrity**The DRP also depends on the recoverability of the backup data and its integrity to avoid restoring corrupt data which could not be used during DR cases. BEC ICT uses software utilities like Recovery manager (RMAN) to backup oracle databases and has capability of detecting corrupt data during backups. The data integrity is also enabled to check for SQL server database backups after backup to validate the backup for database restore and recovery.  **Tier 6: Near-Zero Data Loss**BEC is currently have no Zero Data loss measures in place where ICT critical systems/applications are constantly synchronous or asynchronous mirroring of data to a DR site at remote location. The solution dependent on the availability of active replication software that’s replicates the BEC systems between primary site and secondary sites during business hours. DRP recommends BEC to employ active replication software to adopt Near-zero Data loss and procure replication licenses for active data guard for oracle databases or cloud backup services from vendors.  |
|  |

## EXPECTED RESPONSE TIME

|  |
| --- |
| An expected response time plan defines the procedure of responding to different types of incidents or crisis BEC ICT may experience within defined RTO and RPO defined above. These procedures should address all the major risks BEC ICT might face. It outlines the actions that need to be taken to limit the disruption of service and loss of infrastructure during and after an incident. The expected response time plan includes but not be limited to the following: * 1. Plan activation details, including a clear statement of the circumstances when the plan will be activated and the person authorised to do so (DRP team);
	2. Incident response team details, including key roles and responsibilities;
	3. A communication plan, including key communication methods and timings needed to keep everyone safe;
	4. Contact lists of Interested Parties/Contractors which BEC will need to communicate with during a crisis, including staff and emergency services;
	5. An event log to record information, decisions and actions that should be taken during a crisis
 |

# RECOVERY STRATEGY

## INITIAL RECOVERY

|  |
| --- |
| The initial strategy for Disaster Recovery Plan is to have functional DR site, valid data backups and recovery software licenses in place. These strategy is based on the key business processes and applications defined above on the Dependencies which includes;* AD systems
* Core business applications – Malepa
* Accounting and Finance/Procurement System-ACCPAC
* Payroll – ESS/VIP
* E-mail system

The initial strategy is to restore and recover these critical systems back to operations. However, these depend on the availability of DR site with proper infrastructures like servers, storage, and network availabilities. The DRP team would initially follow the priorities of business application as prioritised according to the DRP and availability of valid recovery software and BEC data backups from Tapes or other External medias. |

## OVERALL RECOVERY STRATEGY

|  |
| --- |
| DRP shall capture all the information that describes the BEC business ability to withstand disaster as well as the processes that must be followed to recover from disaster and/or unexpected event and resume business operations. The overall BEC ICT DRP strategy is developed in such a way that priority or emergency services are fully accessible during the event of disaster. The overall strategy for BEC ICT is shown below; |

## **RECOVERY SCENARIOS**

Data Failure, Critical Recovery Team is unavailable, Business is inaccessible

|  |
| --- |
|  |

# RETURN TO OPERATIONS

|  |
| --- |
|  |