

Bandhan Financial Service Ltd.

Head Office, Kolkata – 700091



Business Continuity Plan

Doc ID: BFSL-BCP-001

Prepared By: Chief Financial Officer
Reviewed By: Managing Director
Recommended By: Company Secretary

Date of Approval of the Board:
Effective Date of this chart:

Revision History

| Date | Version | Description |
|-------------------|----------------|--------------------|
| 29-September-2020 | 1.0 | Base documentation |

1 Introduction

1.1 Purpose

To provide the requirements for preparing a Business Continuity Plan that describes the processing of critical applications in the event of a data centre failure or catastrophic event.

1.2 Scope

This plan applies to critical applications and their operating environments maintained at DC and DR of Bandhan Financial Services Ltd.

1.3 Responsibility

It is the responsibility of management of the BCP Team to ensure that this plan is followed during crisis and tested at least once in a year.

2 Disaster Recovery Plan

2.1 Critical Time Frames and Critical applications

The BCP considers the time that would elapse after the interruption of data processing operations before the organization's critical functions would be interrupted. Additionally, the BCP considers the time involved to restore the critical applications.

Critical Applications

| Sr No | Critical Applications | Time frame required to restore to original state |
|-------|-----------------------|--|
| 1 | Tally ERP | 24 Hours |
| 2 | Network – LAN | 48 hours |
| 3 | Network - Internet | 48 hours |
| 4 | Company Website | 24 hours |
| 5 | | |
| 6 | | |

2.2 Priorities

The BCP provides for priorities in the re-establishment of the processing of critical applications. The following elements are considered in establishing priorities:

1. Nature and extent of a likely disaster
2. The time that reasonably is expected to elapse before normal data processing operations are restored
3. The potential loss to the organization if the processing of the application is not restored in a timely fashion
4. The point at which normal cyclical processing operations might be interrupted.
5. Relative priority to other application DRP's.

2.3 Critical Resources

The BCP identifies the resources required to operate. This includes:

1. people
2. hardware and peripheral equipment
3. the operating system and all systems and utility software
4. network software
5. applications programs
6. data files
7. forms
8. documentation
9. manuals
10. vendors
11. facilities

2.4 Recovering Data Processing Capabilities

The BCP describes the strategy for the recovery of data processing capability. The plan addresses the following:

2.4.1 Recovery Hardware

The plan addresses the arrangement for installing backup hardware in the IT Infrastructure. The following issues are addressed:

1. The elapsed time between loss of capability and installation of hardware
2. The criteria for concluding that the hardware to be installed is compatible with the current environment

3. Requirements for peripheral equipment, software, telecommunications, etc.

2.4.2. Recovery Facility

The plan addresses the arrangement for recovering the data processing capability to an alternate site should the facility (e.g., hot site, cold site) in the Data Centre become unavailable for an extended period. Included are as follows:

1. The elapsed time between loss of the facility and the establishment of operations at the backup facility
2. The criteria for concluding that the time availability and processing capability/capacity at the backup facility are appropriate
3. Required hardware, software, telecommunications, office space, etc.
4. Requirements for travel to the backup site
5. Requirements for carrying out business at an alternate location (e.g., phone service, office space, etc.)
6. Alternate sources of supplies (e.g., required forms) in proximity to the backup facility.
7. Any contracts or agreements with vendors should be described/referenced.

2.4.3 Recovery Data

The plan addresses the programs and data required, identification of special programming or versions of programs that are required and the criteria for concluding that such software is usable should it be required

2.4.4 Recovery Procedures

The DRP addresses the procedures to follow when implementing the plan. These procedures considers the following:

1. Criteria for determining that hardware/software failure and/or destruction of facilities requires implementation of this plan
2. Notification of appropriate personnel and vendors/contractors (the plan should include home telephone numbers)
3. Where the backup programs and files are located and who is authorized to retrieve them
4. Procedures for retrieving stored programs, data files and documentation and reconstructing processing on backup hardware or at the backup facility (requirements for off-site storage of programs, data files and documentation)
5. Where the backup site is and directions to get there
6. Adequate security at the recovery facility

7. Roles and responsibilities for implementing the various elements of the plan (e.g., declaring a disaster, re-establishing telecommunications services, making travel arrangements)
8. Script of all activities in time / order sequence for recovery team.

2.4.5 Recovery Team Members

Identify all recovery teams, team members, and their roles.

BCP Team for Bandhan Financial Service Ltd.

| | Recovery Team | Designation | Contact Number Landline | Contact Number (Mobile) |
|---|---------------|------------------|----------------------------|-------------------------------|
| 1 | | IT Administrator | | |

Business Continuity Manager (BCM): Overall Coordination of recovery team.

BCP Team Members: Duties assigned based on recovery team areas of their responsibility.

3 Testing the DRP

The DRP should establish a testing cycle. Although selected aspects (e.g., reconstruct operating system at the recovery facility) can be tested individually, the DRP should be tested in its entirety. Walk through tests are also acceptable means of testing plans. The tests should be designed to completely test the effectiveness of the DRP in restoring capability on recovery hardware in the data centre or a recovery facility. Appropriate type of test may be selected.

The BCP shall be tested at least once in a year in order to ensure that the plan is valid and effective during adverse situation.

Results of tests to be documented for audit trail and for future drill.

Types of Tests which may conducted are

1. Drills
2. Table Top Tests
3. Functional
4. Full Scale Test

Drill: This tests the individual emergency response functions. These tests are tested under realistic conditions. Here all level of responders is involved. An examples of these drill is fire drill.

Table top test: The basic version seeks to solve problems in a group setting via brainstorming. This test gives a more reality based experience.

Functional Test: This test assesses the allocation of resources and manpower and also evaluates communication across different groups. This test helps in assessing the adequacy of current procedures and policies. Here participants perform actual activities.

Full Scale Test: This test evaluates the operational capability of systems in an interactive manner over a substantial period of time, Presents complex and detailed events in real time. This test mobilizes personnel, resources, emergency response team and equipment. This test can be expensive or may be disruptive to normal operations.

Testing the DRP should consider the following:

3.1 Test Plan

Testing the DRP should be performed according to a test, which should include the following:

1. Test objective (e.g., restore telecommunication capabilities, restore all critical applications at the recovery facility)
2. Schedules
3. Criteria for acceptance
4. Written in script form in time / sequence order.

3.2 Documentation of Test Results

The results of the DRP testing will be documented and retained. The documentation will consist of the following:

1. Description of testing performed
2. Summary of results
3. Problems encountered and how the problems were resolved
4. Required modifications to the DRP as a result of the testing
5. Evidence of appropriate review and approval.

3.3 Testing Team

Identify all Testing team members and their roles. Those having responsibilities in the actual DRP should participate in the testing process if possible.

4 Updating the DRP

The DRP should be reviewed annually by IT strategy committee and updated when changes are made to the hardware, data, facility, procedures or team members defined in the recovery and/or restoration DRP.

5 DRP Storage

A copy of the DRP should be stored in at least one location outside of the data centre. This copy should be easily accessible in the event that the data centre facility become off limits to the recovery team.

6 Backup Storage Types:

6.1 Online Replication

6.2 Storage on Magnetic Tapes

7 IT infrastructure Redundancy

Redundancies are maintained for

1. Power

2. Network / Internet Service Providers