



SQFT Knowledge Services

BUSINESS CONTINUITY PLANNING

Document Revision History

Version	Document No	Date	Brief summary of changes	Prepared By	Approved By
1.0	SQFT/BCP/PO L/013	1-Mar-2019	Initial version created	K. Gokhul	S.Nandhini
1.0	SQFT/BCP/PO L/013	1-Mar-2020	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/BCP/PO L/013	1-Mar-2021	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/BCP/PO L/013	1-Mar-2022	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/BCP/PO L/013	22-Apr-2022	Added Checklist for BCP	K.Gokhul	S.Nandhini
1.2	SQFT/BCP/PO L/013	03-Jan-2023	Reviewed and updated the policy for Privacy management systems	K.Gokhul	S.Nandhini
1.2	SQFT/BCP/PO L/013	1-Mar-2023	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.3	SQFT/BCP/PO L/013	01-Apr-2023	Updated Employee details in Clause 5	K.Gokhul	S.Nandhini
1.3	SQFT/BCP/PO L/013	01-Apr-2023	Updated Employee details in Clause 5	K.Gokhul	S.Nandhini
1.4	SQFT/BCP/PO L/013	29-Feb-2024	Updated Employee details in Clause 5	K.Gokhul	S.Nandhini

1 PURPOSE	3
2 SCOPE	3
3 BCP POLICY	4
4 ORGANIZATION	4
5 IDENTIFYING CRITICAL FUNCTION:	5
6 BCP TEAM ROLES AND RESPONSIBILITIES:	5
7 PROVIDING TRAINING AND AWARENESS:	7
8 DOCUMENTING TEAM DETAILS:	7
9 BIA BUSINESS IMPACT ANALYSIS:	7
9.1 RECOVERY TIME OBJECTIVE	8
9.2 RECOVERY POINT OBJECTIVE	8
10 BUSINESS CONTINUITY PLAN	8
SITE OUTAGE	8
11 DISASTER RECOVERY TEST SCHEDULE	8
12 CRITICAL INFORMATION ASSETS	9
13 TESTING OF PLANS	9
14 BACKUP DATA	10
15 OFFICE EQUIPMENT, FURNITURE AND SUPPLIES	11
16 ASSOCIATED DOCUMENT	11

1 PURPOSE

SQFT KS business relies more on the mind power/skills of employees. Information in the form of data is less critical except for some key departments.

Business continuity planning is the process of making certain that business functions, handled by SQFT KS remain uninterrupted through time. It involves successfully mitigating risks from natural, manmade, or environmental threats, and building resilient arrangement that can overcome the risks identified during routine assessment.

2 SCOPE

Since all major operations and business dealings essential for the development of , it is agreed to kick off the implementation of business continuity plan from its Chennai location located at the following address

Location 1: 34 /120, New St, Muthialpet, George Town, Chennai, Tamil Nadu 600001

Location 2: No: 103 GNT Road, Sholavaram, Tiruvallur - 600067

The scope includes all operations / functions currently running in the above location.

Business Continuity Plan is designed to create a state of readiness that will provide an immediate response to any of the following incident scenarios:

- Any incident causing physical damage such as fire, smoke, water damage.
- Any incident which indirectly affects facility access such as storm, emergency building evacuation due to bomb threat, or external threat such as fire to any of the floors of SQFT KS building.
- Any environmental incident such as poor ventilation, heating or cooling problems that would jeopardize operations.
- Impending or unexpected regional disaster such as storm or flood.
- Any external incident, which potentially could cause a business interruption, such as loss of electrical or telecommunications service.
- Any incident that causes a serious outage to
 - ❖ Use of or access to the building.
 - ❖ Power
 - ❖ Communication lines
 - ❖ Critical Applications & Data base Servers
 - ❖ ISP Links
 - ❖ Computing resources/LAN
 - ❖ Human resources

3 BCP POLICY

BCP Policy illustrates the significance of SQFT KS's declaration in establishing, implementing and maintaining BCMS. The policy is approved and circulated to all stake holders. The policy is also published in SQFT KS's Intranet system. Key points of the BCP Policy are as mentioned below

- Annually review the Risk Assessment including periodic maintenance of the Business Impact Analysis.
- Periodically update the Business Continuity plan to ensure currency of information, and response strategies. The plan must be reviewed for possible updating within 30 days of any major operational or system changes that will have a material effect on the contingency strategy of any department / unit.

Undertake exercises for training and evaluation purposes of the Business Continuity Plan each year or within 30 days of any major operational or system changes that will have a material effect on the contingency strategy of any department / unit.

Management responsibilities

Managers of SQFT KS must ensure that the key functions for which they have responsibility are able to continue following major disruptive events and that arrangements are in place to achieve this. This requires the proactive development, maintenance and devolution of business continuity planning within their areas. Managers are expected to encourage the active participation of employee in business continuity issues and must ensure that key personnel are able to perform competently during a major disruptive event.

SQFT KS must;

1. Complete a periodic Risk Assessment or more detailed Business Impact Analysis
2. Manage risks in accordance with this policy

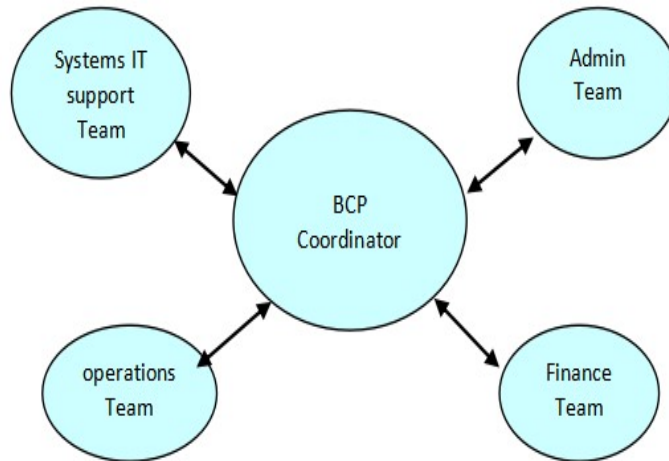
Ensure that the Business Continuity Plan in their area of influence and control is exercised on schedule.

4 ORGANIZATION

The Business Continuity organization's primary duties are:

- To protect employees and information assets until normal business operations are resumed.
- To ensure that a viable capability exists to respond to an incident.
- To manage all response, resumption, recovery, and restoration activities.
- To support and communicate with employees, system administrators, vendors, security personnel, and managers.

- To accomplish rapid and efficient resumption of time-sensitive business operations, technology, and functional support areas.
- To ensure regulatory requirements are satisfied.
- To exercise resumption and recovery expenditure decisions.
- To streamline the reporting of resumption and recovery progress between the teams and management of each system.



5 IDENTIFYING CRITICAL FUNCTION:

SQFT KS as an organization consist of 8 Full Time working together in Location 1 and 6 Full Time in Location 2 achieving its business mission and objective. The critical functions are identified in each department and Business impact analysis is done.

- Operations
- Finance
- Administration
- IT
- BCP coordinators

6 BCP TEAM ROLES AND RESPONSIBILITIES:

The BCP team consists of BCP coordinator and one or more members from Operations, system support, administration, finance and offsite. Each team will have a roster and task list of actions and responsibilities, as outlined below.

BCP coordinator

- Monitor and coordinate Business continuity Plan, training, awareness, exercises and testing.
- Coordinate strategy development with other teams.
- Work closely with other team leaders.
- In-charge to declare about the disaster and invoking a BCP.
- Informs the team/ Team leaders about the initiation of the BCP.
- Informs the management about the BCP initiation.
- Get budgetary approvals from the management for requirements on BCP.
- Prepares reports and submit them to management.
- Implement identified improvements from test/actual data.
- Initiates measures to bring to normalcy.
- Declare the normalcy after BCP.

Operations Team

- Coordinate with systems support team to establish the operations at backup site.
- Define the requirements and submit for approval from ISPSC , through the BCP coordinator.
- Coordinate with systems support and admin team for establishing the requirements at offsite.
- Inform other teams about the requirements in both logistics and technical.
- Work in conjunction with other teams involved in BCP testing.
- Coordinate with client in the event of BCP initiation.
- Once normalcy is declared, establish the normal operations at original site with all the data.

Systems and IT Support Team

- Help in defining the requirements with the Operations Team.
- Coordinate in restoring data and communication links between user, computers and client.
- Keep the backup systems and software ready in the event of disaster.
- Periodic testing of hardware, software and backups at offsite.
- Involved in testing the BCP.
- Secure Storage of the External Hardisk
-

Admin Team

- Responsible for contacting the vendors, BCP teams.
- Provide the voice communication facilities.
- Logistics support.
- Shifting the people to off-site.
- Coordinate with transporting agency (if required).
- Inform the employees families in the event of disaster.
- Testing of all emergency equipment such as power, lighting etc.
- Shifting the backup tapes/software to offsite securely.
- Other miscellaneous arrangement such as food etc.

Finance Team

- Arrange for finance.
- Prioritize and manage receivables and payables.

7 PROVIDING TRAINING AND AWARENESS:

Preliminary awareness and training is provided to the qualified/identified employees of SQFT KS who are the key personnel getting involved in BCP process. The awareness is given at a broader level covering the most critical activities of BCP like BIA, Testing, and Maintenance etc.,

8 DOCUMENTING TEAM DETAILS:

SQFT KS has formed four teams for smooth execution of BCP process during any real time disaster or emergency. The teams are as given below.

1. BCP Team or Information Security and Privacy Forum
2. Business Invocation Team
3. Functional Recovery Team

BCP coordinator is the manager of BCP Team and BCP document. All the teams will be reporting to him in case of any real time emergency. He/she will be the one point contact for all the BCP activities.

To know the name and contact number of the all the team member, refer sheet "BCP Contact Details.xls"

9 BIA BUSINESS IMPACT ANALYSIS:

The BIA is one of the most important steps in the overall BCP process. The data gatherer is pivotal to identifying key business issues and justifying to executives the resources needed.

The BIA determines the financial exposures and operational impacts resulting from a major disruption of services. It will provide with

- The identity of its time-sensitive business operations and services.
- An analysis of the organization's financial exposures and operational impacts
- The time-frames in which time-sensitive operations, processes and functions must resume.
- An estimate of the resources necessary for successful resumption, recovery and restoration.

The BIA provides the rationale and cost justification for risk mitigation and response, resumption, recovery and restoration-related decisions.

After completing BIA at the head office it has been identified that the following are the most critical functions/processes irrespective of all the departments in SQFT KS

- Internet Connectivity
- Firewall (VPN Connectivity)

The result of BIA with the list of critical processes / functions / applications / systems is documented in the Business Impact Analysis. This sheet eventually captures the Recovery Time Objective /Recovery Point Objective of each critical processes / functions / applications / systems of all departments respectively.

9.1 RECOVERY TIME OBJECTIVE

- The least RTO expected is 4.0 Hr (i.e. four hours) for basic infrastructure.
- In IT infrastructure LAN / WAN/ Internet/Mail has an expected RTO of 4 hours
- Maximum affordable downtime is 96 Hrs to 1 week for various less critical activities of respective departments.

9.2 RECOVERY POINT OBJECTIVE

- The minimum RPO specified is 4 Hrs (i.e. two hours) for knowledge processing activities
- For all other services the expected RPO is 1 day i.e. restoration of the previous day's backup is sufficient

10 BUSINESS CONTINUITY PLAN

SITE OUTAGE

Scenario: Business functions affected because of non-availability of site or site is unreachable due to some or the other reason.

Plan:

For Location 1 and 2 shall be treated as the alternate site and Vice Versa. The addresses are given below.

In this scenario BCP Coordinator will be issuing further instructions as per the BCP discussions with the management.

11 DISASTER RECOVERY TEST SCHEDULE

Sl. No	Disaster Condition	Impact	Test Schedule
1	Fire Drill	High	Every 6 Months
2	Server	High	Every Year
3	Network Devices	High	Every 6 Months
4	Power	High	Every 6 months
5	Air Conditioning in Server Rooms	Medium	Every 6 months
6	UPS	High	Every 6 months
7	System accessibility	Medium	Every 3 months

- These tests are to be conducted with prior scheduled outage notification to Operations.

- During the test schedule, services as given in the table will remain down, as the failure condition will be simulated. Technology and Operations should test the services and note the test results, experiences, and suggestions.
- Every Service, which is expected to have an impact on the test condition, needs to be tested individually. Test conditions should be tabulated.
- Required configuration and data backup to be taken before simulating the problem condition.

Objectives of the tests

- To be prepared to meet the failure conditions confidently during live operation.
- Get first-hand experience on the time taken to recover.
- Identify the procedures to be followed to recover from known failure conditions.
- To proactively identify unexpected errors and problems during recovery.

12 CRITICAL INFORMATION ASSETS

Scenario: Business functions affected due to failure of any one of the critical devices such as servers, router, firewall, leased line, switches etc.

13 TESTING OF PLANS

Test plans shall be developed for various scenarios and testing shall be conducted according to the schedule maintained as per Section 11

BCP Notification

COO for the locations where the critical components of SQFT KS systems are located should be provided with the telephone numbers of SQFT KS BCP team members Team Contact List Upon notification, the team will meet for the purpose of conducting initial incident assessment and issuing advisory reports of status to COO and Top management. If the functional managers, other security team members or BCP Coordinator has determined that the building cannot be entered, the alternate meeting place will be at Offsite office.

Contact list of emergency services.

The contact information of external agencies for e.g. Govt. administrative authorities, fire brigades, Business Continuity service providers, agencies, etc shall be maintained as per Emergency Contact List

Vendors and Consultants

the contact list of all vendors and consultants shall be compiled and maintained a vendor contact list , so as to expedite the recovery process.

Employee contact information

The contact information of employees shall be maintained as per Employee Contact Information. In the event of a disaster, a lack of specific personal data, including home addresses, cell phone numbers, and alternate contact information, could result in the inability to locate and contact key personnel and team members. This personnel database should be maintained and updated continuously. This database may be maintained by the BCP co-coordinator who will take care that the information contained therein remains current and accessible and is available as part of the Business continuity plan.

14 BACKUP DATA

The important asset in SQFT KS is its data and information. Data and information processing are a major reason for the existence of projects. Moreover, all of the systems are dependent on the preservation of data, including project manuals and procedural documentation. In order to minimize the impact of a disaster, it is extremely important to protect data and information.

Effective procedures to perform full data backups on a regular basis must be implemented.

In case of a disaster, an alternate site shall be prepared, by the systems support team with the help of other BCP teams.

Vital Records/Documentation

Vital records and important documentation shall be backed up and stored off site. Vital records are any documents or documentation that is essential to the operations of an organization, such as personnel records, software documentation, legal documentation, legislative documentation, benefits documentation, etc.

Maintenance of backups and documentation offsite.

A copy of the backups shall be stored off site in an environmentally controlled storage facility. A back up copy must be stored safely and should include documents such as security plans, Business Continuity plans, risk analysis, and security policies and procedures. Additional copies may be necessary for some documentation, such as Business Continuity plans, which should be easily accessible in the event of a disaster.

It is recommended that copies of the Business Continuity Plan be distributed to SQFTKS Management, Business Continuity Plan Coordinator, and Team Leaders for safekeeping.

Documentation should be duplicated either in hard copy or compatible media format and stored in the safe location. The original primary on-site unit retains the original copies of all information. Updates to documentation should be done as-required basis, under the control of the responsible team. Off-site documentation should include technical and operational documentation.

All the files are maintained in safe location:

Detailed manuals specifying how their functional responsibilities are to be discharged in the event of their unavailability are to be developed. This is especially important for key personnel. Copies of these manuals should be kept off-site with other documentation.

15 OFFICE EQUIPMENT, FURNITURE AND SUPPLIES

Admin shall review the supply needs and coordinate and develop a revolving emergency inventory of workspace and survival supplies for immediate use in the event of a disaster. The revolving inventory of workspace supplies should include not only basic essential workspace supplies like pens, pencils, note pads, and paper, but also SQFT KS specific forms.

16 ASSOCIATED DOCUMENT

- BCP Drill Report (SQFT/BCP/FMT/026)

End of Document