EC No. 89/ DoS - 07/ 2024 10 May 2024

Ref. No. NB. HO. DoS. Pol. / 657 / J-1 / 2024-25

The Chairman, Regional Rural Banks
The Managing Director, All State Cooperative Banks
The Managing Director/ Chief Executive Officer,
All District Central Cooperative Banks

Madam/Dear Sir,

Guidance Note on Business Continuity Plan (BCP)

Please refer to our letter No. NB.DoS.HO.POL./5390/J-1/2009-10 (Circular No. 69/DoS - 03/2009-10) dated March 30, 2010, wherein banks were advised to implement a robust Business Continuity Plan (BCP) to mitigate the impact of operational risks due to the rising complexity of financial products and the expanded use of technology with its increased sophistication. This advisory aimed to guide banks in enhancing their risk management framework.

2. The importance of implementing strong business continuity plan has grown significantly due to increased supervisory expectations and heightened complexity in the banking ecosystem. Accordingly, it has been felt that there is a need to revisit guidelines on business continuity plan to mitigate the risks in the event of disruptions in SEs. They should have a keen awareness of the need to identify critical business functions and evaluate vulnerabilities and threats as well as to determine that they have a sound organisational framework and Corporate Governance for effective implementation of BCP. On these lines, guidance note on BCP has been revised.

3. SEs are advised to develop a robust BCP to enhance risk mitigation strategies so that they can better prepare for tackling different threats and risks. They should develop comprehensive risk management plans that cover all areas of their operations, including financial risks, technological risks, environmental risks, human resources risks, etc. SEs must ensure that the BCP methodology covers the following:

a) A Business Impact Analysis (BIA) that identifies critical business functions and establishes Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

b) Structured risk assessment based on comprehensive business impact analysis, considering all critical bank functions, including routine transactions, payment systems, and online banking.

c) Risk monitoring which involves BCP testing at regular intervals, independent audit and review of BCP and updating BCP based on changes in personnel and the internal/external environments.

d) BCP should address procedural, infrastructure, human resources, and technology aspects to effectively mitigate wide-area disasters and ensure operational resilience.

e) Regular review and updating of BCP based on audit findings and departmental feedback.

4. We advise that all RRBs, scheduled StCBs, and other SEs with over Rs. 3000 crore in business size by 31 March 2024, will undergo E-CAMELSC based supervisory approach based on their financial position by the same date. The remaining banks will be brought under E-CAMELSC approach in a phased manner. The SEs covered under E-CAMELSC based supervisory approach are advised to put in place effective and robust business continuity plan as envisaged in the guidance note by ***30 September 2024.***

5. Remaining banks are advised to put in place effective business continuity plan framework by **31 March 2025.**

6. We advise that a copy of this circular may be placed before the next meeting of the Board of Directors of your bank so as to take a suitable decision on implementation of the guidelines in your bank.

7. Please acknowledge the receipt of this circular to NABARD Regional Office in your State/ UT.

Yours faithfully

Sd/-
(Sudhir Kumar Roy)
Chief General Manager

Encl: Guidance note

Main Document

Document title	Guidance Note on Business Continuity Plan
Drafted by	Department of Supervision
Date of approval	26 March 2024
Document classification	External
Document no. / Version no.	2.0

Version history

Version No.	FY	Changes / Comments	Changed by
1.0	2009-10	New policy	-
2.0	2024-25	Revised	Department of Supervision

Version Approval

Version No.	Date of approval	Changes / Comments	Approved by
1.0	2009-10	New policy	Board of Supervision
2.0	2024-25	Revised	Board of Supervision

References

Sr. No.	Reference	Reference No.
1	Operational Risk Management-Business Continuity Planning	Circular no. 69 / DOS-09/ 2010, Ref. no. NB.DoS.HO.POL./5390/J-1/2009-10 dated 30 March 2010

Guidance Note
on
Business Continuity Plan

NABARD

Table of Contents

1. Introduction 1

2. Objectives of BCP 1

3. Advantages of BCP 1

4. BCP Organisation structure and Corporate Governance 2

5. BCP Methodology 5

6. Business Impact Analysis (BIA) 6

6.1 Recovery Time Objectives 7

6.2 Recovery Point Objective 7

7. Risk Assessment 8

8. Risk Monitoring 10

9. Testing of BCP 10

9.1 Testing Techniques 11

9.2 Review /feedback of the BCP 12

10. Procedural aspects of BCP 12

11. Infrastructural Aspects of BCP 12

12. Human Resources Aspects of BCP 13

13. Technology Aspects of BCP 13

13.1 Disaster Recovery 13

Annexure 1 18

Annexure 2 19

Annexure 3 20

Annexure 4 21

Annexure 5 22

Annexure 6 23

Annexure 7 24

Guidance Note on Business Continuity Plan (BCP)

1. Introduction

The increasing complexity of financial products and the greater reliance on advanced technology have made operational risks more significant in the banking industry. Given the rise in complex financial products and the expanded use of technology, it is essential to establish comprehensive Business Continuity Plan (BCP) guidelines that address key aspects such as people, processes, and technology in the banking environment.

Business Continuity Plan (BCP) is a key pre-requisite for minimising the adverse effects of one of the important areas of **operational risk** – business disruption and system failures. BCP is aimed at uninterrupted customer services, backup and restoration procedures, effectiveness of the backups, disaster avoidance facilities, recovery and fallback procedures in case of natural disasters.

A BCP is a comprehensive, written document developed to maintain and/or resume business operations, including service to customers, in the event of any disruption in the banking service.

2. Objectives of BCP

The main goal of a business continuity plan is to minimise losses during disruptions. This includes minimising financial losses, operational losses, and any other losses that could occur due to a disruption in service or operations. Another key objective of a BCP is to ensure business continuity in the face of any type of disruption. This means that banks must be prepared for any potential disruption to continue operations with minimal disruption. The third objective of a BCP is to enhance risk mitigation strategies so that banks can better prepare for tackling different threats and risks. Organisations should develop comprehensive risk management plans that cover all areas of their operations, including financial risks, technological risks, environmental risks, human resources risks, etc.

A well laid out BCP can minimise the impact of the disaster and minimise the **operational, financial, legal, and reputational risks** as also other things arising out of such a disaster. The ability of the bank to overcome difficult situation and resumption of the activities when disaster strikes, is critical to the customer confidence, growth and survival.

3. Advantages of BCP

BCP is the process of evaluating potential weakness and planning how to deal with what could possibly go wrong in case any disaster strikes. It offers the management a chance to get better understanding of their business thereby ultimately helping an organisation identify ways to strengthen any shortcomings, even in areas that had previously gone unnoticed.

BCP can strengthen the organisation not only against large-scale problems, but also help make smaller problems that might have caused continuity interruptions through detailed planning. A BCP helps protect the Organisation's image, brand, and reputation. It can significantly minimise the loss, in case hit by a disaster.

4. BCP Organisation structure and Corporate Governance

The ultimate responsibility of BCP rests with the Board of Directors and the top management. Board should provide top management clear guidance and direction in relation to BCP. Senior Management is responsible for overseeing the BCP process which includes:

a. Determining how the institution will manage and control identified risks.

b. Allocating knowledgeable personnel and sufficient financial resources to implement the BCP.

c. Prioritising critical business functions.

d. Designating a BCP Coordination Committee who will be responsible for the Business Continuity Management.

e. The top management should annually review the adequacy of the institution's business recovery, contingency plans and the test results and put up the same to the board.

f. The top management should consider evaluating the adequacy of contingency planning and their periodic testing by service providers, whenever critical operations are outsourced.

g. Ensuring that the BCP is independently reviewed and approved, at least annually.

h. Ensuring employees are trained and aware of their roles in the implementation of the BCP.

i. Ensuring the BCP is regularly tested on an enterprise-wide basis.

j. Reviewing the BCP testing programme and test results on a regular basis.

k. Ensuring the BCP is continually updated to reflect the current operating environment.

4.1 BCP Head or Business Continuity Co-ordinator

A senior official needs to be designated as the head of BCP activity or function. His or her responsibilities include:

a. Developing of an enterprise-wide BCP and prioritisation of business objectives and critical operations that are essential for recovery.
b. Business continuity planning to include the recovery, resumption, and maintenance of all aspects of the business, not just recovery of the technology components.
c. Considering the integration of the institution’s role in financial markets.
d. Regularly updating business continuity plans based on changes in business processes, audit recommendations, and lessons learned from testing.
e. Following a cyclical, process-oriented approach that includes a business impact analysis (BIA), risk assessment, risk monitoring and testing of BCP.
f. Considering all factors and deciding upon declaring a “crisis”.

4.2 BCP Committee

Since electronic banking has functions spread across more than one department, it is necessary that each department understands its role in the plan. It is also important that each gives its support to maintain it. In case of a disaster, each must be prepared for a recovery process, aimed at protection of critical functions.

Hence, a committee consisting of heads/senior officials from departments like HR, IT, Legal, Business and Information Security needs to be instituted with the following broad mandate:

a. To exercise, maintain and to invoke business continuity plan, as needed.
b. Communicate, train and promote awareness.
c. Ensure that the BCP fits with other plans and requirement of authorities concerned.
d. Budgetary issues
e. Ensure training and awareness on BCP to concerned teams and employees.
f. Co-ordinating the activities of other recovery, continuity, response teams and handling key decision-making.
g. Other functions entail handling legal matters evolving from the disaster and handling public relations and media inquiries.

4.3 BCP Management Teams

There needs to be adequate teams for various aspects of BCP at central office, as well as individual controlling offices or at a branch level, as required. Among the teams that can be considered based on need, are the incident response team, emergency action and operations team, team from particular business functions, damage assessment team, IT teams for hardware, software, network support, supplies team, team for organising logistics, relocation team, administrative support team, coordination team.

Sample guidelines for committees or teams for BCP are provided below:

BCP people or Group	HR
Topic	Ideas
1. Roles, responsibilities and authorities	• Communication to staff and onsite contractors • Fatalities handling or counselling • Resourcing • Maintain staff and contractor's database
2. Necessary competencies	• Documentation planning • Change management • HR CIPD (Chartered Institute of Personnel and Development) certification • Health and safety
3. Approach to training needs analysis	• Counselling • Training scenarios • Desktop exercises • Find out if managers know responsibilities for embedding BCP in community
4. Appropriate training	• Table top • Scenario walkthroughs • Full exercises
5. Ways of measuring necessary competence	• Audits • Practical exercise • Live invocation
6. Suitable records of education, training, skills, experience and qualifications	• Past exercise reports

BCP people or group	BCP Teams
Topic	Ideas
1. Roles, responsibilities and authorities	• Set out in plan • Assigned to position
2. Necessary competencies	• Knowledge of business • Understanding impact • Ability to analyse information • Leadership
3. Approach to training needs analysis	• Interview • Previous experience • Skills required • Scenario-"what would you do if" impact analysis
4. Appropriate training	• Sharing knowledge: ○ Senior staff ○ Junior staff ○ External • Exercise
5. Ways of measuring necessary competence	• Assess practical • Review capability following event
6. Suitable records of education, training, skills, experience and qualifications	• Past exercise records

BCP people or group	**BCP Committee**
Topic	Ideas
1. Roles, responsibilities and authorities	• Authorities to exercise, maintain and to invoke plan (if specified) • Communication, training and promoting awareness • Fits with other plans/ authorities • Budget • Ensure others are trained
2. Necessary competencies	• Understanding of business and business continuity framework • Proficiency and expertise in own function • Trained • Ability to communicate
3. Approach to training needs analysis	• Corporate approach/strategy for BCP • How is BCP implemented • Include deputies • Capability to exercise skills
4. Appropriate training	• Same as the topic Approach to training needs analysis

5. BCP Methodology

This document outlines the essential requirements for a BCP that should be adhered to. The responsibility for developing detailed BCP components tailored to the specific activities, systems, and processes of each bank rests with the board and senior management.

BCP methodology should include:

Phase 1: Business Impact Analysis (BIA)

1. Identification of critical businesses, owned and shared resources with supporting functions to come up with the BIA.
2. Formulating RTO, based on BIA. It may also be periodically fine-tuned by benchmarking against industry best practices.
3. Critical and tough assumptions in terms of disaster, so that the framework would be exhaustive enough to address most stressful situations.
4. Identification of the RPO for data loss for each of the critical systems and strategy to deal with such data loss.
5. Estimation of resource requirements for the processes that are affected during any disaster.

Phase 2: Risk Assessment

1. Structured risk assessment based on comprehensive business impact analysis. This assessment considers all business processes and is not limited to the information processing facilities.
2. Risk management by implementing appropriate strategy/ architecture to attain the bank's agreed RTOs and RPOs.

3. Impact on restoring critical business functions, including customer-facing systems and payment and settlement systems such as cash disbursements, ATMs, internet banking, mobile banking, IMPS, RTGS, NEFT or call centres.
4. Dependency and risk involved in use of external resources and support.

Phase 3: Determining Choices and Business Continuity Strategy

1. BCP should evolve beyond the information technology realm and must also cover people, processes and infrastructure.
2. The methodology should be effective for the safety and well-being of people in the branch / outside location at the time of the disaster.
3. Define response actions based on identified classes of disaster.
4. To arrive at the selected process resumption plan, one must consider the risk acceptance for the bank, industry and applicable regulations.

Phase 4: Developing and Implementing BCP

1. Action plans (defined response actions specific to the bank's processes), practical manuals (do's and don'ts, specific paragraphs customised to individual business units) and testing procedures.
2. Establishing management succession and emergency powers.
3. Compatibility and co-ordination of contingency plans at the level of both the bank and its service providers.
4. The recovery procedure should not compromise on the control environment at the recovery location.
5. Having specific contingency plans for each outsourcing arrangement based on the degree of materiality of the outsourced activity to the bank's business.
6. Periodic updating to absorb changes in the institution or its service providers. Examples of situations that might necessitate updating the plans include acquisition of new equipment, upgradation of the operational systems and changes in

    a. Personnel
    b. Addresses or telephone numbers
    c. Business strategy
    d. Location, facilities and resources
    e. Legislation
    f. Contractors, suppliers and key customers
    g. Processes–new or withdrawn ones
    h. Risk (operational and financial)

6. Business Impact Analysis (BIA)

It involves the identification and analysis of various critical businesses, resources owned and shared and potential vulnerabilities, threats which should be considered for BIA. BCP should be for both prevention and control, keeping in view the magnitude of the risk and probability of occurrence. Vulnerability assessment and reviews should be a part of the internal control of the Bank subject to periodical updating by the Internal Audit Department. It involves formulating the RTO and the RPO. The following impact analysis scale can be used for evaluating different processes on the basis of the nature and criticality of their functions.

Score	Level	Consequence Type	Impact
1	Insignificant	Financial	Financials are hardly impacted
		Operational	Operations are hardly impacted
		Reputation	Very mild impact on public attention
		Legal and Regulatory Compliance	Very minor legal issue. No penalties
2	Low	Financial	Financials are mildly impacted
		Operational	Operations are mildly impacted
		Reputation	Mild impact on public attention
		Legal and Regulatory Compliance	Minor legal issue. No penalties
3	Moderate	Financial	Financials are moderately impacted
		Operational	Operations are moderately impacted
		Reputation	Medium impact on public attention
		Legal and Regulatory Compliance	Moderate breach of the law. Moderate penalties
4	High	Financial	Financials are significantly impacted
		Operational	Operations are significantly impacted
		Reputation	Significant impact on public attention
		Legal and Regulatory Compliance	Major breach of the law. Considerable penalties
5	Major	Financial	Financials are severely impacted
		Operational	Operations are severely impacted
		Reputation	Severe impact on public attention
		Legal and Regulatory Compliance	Severe breach of the law. Large penalties

6.1 Recovery Time Objectives

Recovery Time Objective (RTO) is defined as the maximum time business can survive without IT systems. The minimum delay for resuming the functions after the impact of an event. This would vary from event to event. The ideal minimum recovery time referred to as RTO in case of various probable events affecting the bank's business processes, based on the business impact analysis, is given in **Annexure 1.** Depending on this time, the BCP has to be planned and recovery process should commence.

Some of the infrastructure related incidents and indicative suggestions to help the branches in preparation of the BCP are given in the **Annexure 2, 3, 4 and 5.**

6.2 Recovery Point Objective

Recovery Point Objective (RPO) is defined as the point in time to which the data can be recovered. In simple words, how much data can we afford to lose. Since we deal with customers' data and cannot afford to lose transactions, which will affect our credibility and lead to reputation risk, the RPO is also ideally should be zero at least in CBS scenarios. It may vary depending upon the technological progress of the bank.

7. Risk Assessment

The risk is to be assessed on the basis of the comprehensive business impact analysis. This assessment should take into account all the functions of the bank and not limited to Information Technology alone. This involves restoring all critical functions like routine business transactions, payment and settlement systems, cash disbursements, ATMs, internet banking, etc.

7.1 Threat / Vulnerability /Risk Analysis

- **A risk** is the potential that a given threat will exploit vulnerabilities to cause loss/damage to assets. It is a function of the impact of the undesirable event and the probability of the event's occurrence.
- **Vulnerabilities** are weaknesses associated with the assets, which in most cases are lack of internal controls. Vulnerability in itself does not cause harm until exploited.

7.2 Types of Vulnerabilities

- Lack of environmental security
- Lack of physical security
- Lack of network access control
- Lack of network monitoring for intrusion detection
- Lack of system maintenance - Machines and equipment are prone to break down, if not maintained properly. With the advent of Core Banking Solution (CBS), all the data of the bank is stored in one centralised place called data centre (DC). It has a host of networked machines (hardware and software included). Notwithstanding the good care and maintenance of the assets, breakdowns cannot be ruled out.
- Lack of controls in back-up, storage and restoration processes
- Lack of anti-virus measures
- Inappropriate location of the Data Centre

7.3 Threats

Threats are internal or external factors that could cause damage / harm / loss to assets and cause disruption in the business. Threats can be accidental or deliberate.

Types of Threats

Some of the major types of threats are as under:

7.3.1 Natural calamities

- *Flash Floods* - Activities such as keeping the important documents on top of the table /removing the documents from the vault to a safe place is to be initiated. Once the premises are cleaned after water recedes, work should resume promptly, with priority given to critical services.
- *Earthquake* - Necessary precautions should be taken especially in earthquake prone areas. If the premises cannot be put to use immediately,

after the earthquake, a temporary arrangement in the vicinity to be made and the branch functioning started with alternate set-up. Electrical connections should be restored by a proper technician before start of the same to avoid short circuits/failures. Branch should identify such a suitable place and proper information / display should be made available to public. After the earthquake in case of need, necessary inspection of the safety of building is to be done by an Engineer.

- *Fire outbreak* - Smoke detectors and fire alarms should be installed and they should be maintained on a regular basis. Combustible articles should not be used or stored in the installation. They should be tested periodically for proper functioning. Fire exits should be clearly marked and should remain unobstructed. Fire insurance policies should be kept current. Staff should be aware of the actions to be taken by them in case of a fire breakout. Fire drill should be done at periodic intervals.

7.3.2 Human interference

- *Theft or Sabotage*
- *Human error in processing*
- *Bomb threat*- After the incident, services to be commenced after cleaning the premises. The data stored and kept elsewhere has to be collected and installed in a new hardware and critical functions commenced in the beginning. An assessment of the damage caused by such act is to be taken before starting the work.
- *Effluent / Gas Leakage*-People should be told to vacate the place immediately. Keep the doors and windows open. Restore normalcy the moment the area is found fit for human occupation.
- *Physical Access Controls*- Proper access control register should be maintained properly logging the names of the personnel accessing the DC/server rooms. There should be appropriate exit control measures to check/prevent removal of sensitive data or equipment / component from the DC/branch. Some of the items to be covered in the plan are like electronic/manual locks on the doors of the system room, authentication controls (through password control or code number or biometrics) to allow only authorised personnel to enter system room or other sensitive areas within the DC. Duplicate copies of key codes or keys that may be used to surmount physical access controls in emergency should be obtained and maintained securely in sealed envelopes, to be opened only in the event of an emergency. These sealed envelopes should be maintained with the head of the installation, who will arrange for storing them securely at prominent places with instructions for retrieval.

7.3.3 Technology failures

- *Infrastructure-related breakdowns*
- *Hardware failures*
- *Software failures*
- *Network component failure*
- *Network intrusion*
- *Virus attack*

- *System failure*
- *Communication link failure*
- *Power outage* - Power and surge protection requirements should be identified, and adequate surge protection devices should be installed. UPS system of adequate load capacity should be installed. UPS system and the batteries should be regularly maintained. Emergency generators should be installed to avoid disaster due to prolonged power interruption. Diagram of electrical/LAN cabling should be displayed at a prominent place at the DC for information & awareness of all concerned. LAN cabling should be kept separated from electrical cables.

(Please see ***Annexure 6*** *for checklist of security precaution at bank branches and* ***Annexure 7*** *for emergency service listing for bank)*

Note*: It may not be possible to give all the disaster /events which may occur which will disrupt the smooth functioning of the bank since it depends upon the geographical location of the branch/bank and expected calamites /vulnerabilities. Some of the items are mentioned as guidance. While preparing the BCP, the location of the place and various events which can happen should clearly be mentioned alongwith the action to be initiated.* ***(Please see the annexure for indicative instances.)***

8. Risk Monitoring

Risk monitoring is an essential part of BCP. All the functional departments in the bank shall ensure that its BCP is viable through:

- Testing the BCP at least periodically say half-yearly/annually.
- Independent audit and review of BCP, whenever called for.
- Updating the BCP based upon changes in personnel and the internal / external environments (including technological advancements and based on periodic feedback).
- BCP Committee at head office shall be responsible for ensuring ongoing monitoring.

9. Testing of BCP

Testing of BCP should include all aspects and constituents of a bank i.e., people, processes and resources (including technology). In case of incorrect assumptions, oversights or changes in equipment or personnel, the BCP may not work. BCP tests should ensure that all members of the recovery team and other relevant staff are aware of the plans. The test schedule for BCPs should indicate how and when each component of a plan is to be tested. Some of the measures which can be taken are as follows:

1. Banks should involve their internal auditors/IS auditors to audit the effectiveness of BCP.
2. Bank should consider having a BCP drill planned along with the critical third parties, to provide services and support to continue with pre-identified minimal required processes.
3. Banks should also be periodically moving their operations - including people, processes and resources (IT and non-IT) - to the planned DR site in order to

test the BCP effectiveness and also gauge the recovery time needed to bring operations to normal functioning.

4. Banks should consider performing the above test without movement of bank personnel to the DR site. This will help in testing the readiness of alternative staff at the DR site.

A variety of techniques should be used to provide assurance that the plan(s) will operate in real life.

9.1 Testing Techniques

The following techniques are generally adopted for testing the BCP

- *Simulations testing* - It is when participants choose a specific scenario and simulate an on-location BCP situation. It involves testing of all resources like people, IT and others, who are required to enable the business continuity for a chosen scenario. The focus is on demonstration of capability, including knowledge, team interaction and decision-making capabilities.
- *Component testing:* This is to validate the functioning of an individual part or a sub process of a process, in the event of BCP invocation. It focuses on concentrating on in-depth testing of the part or sub-process to identify and prepare for any risk that may hamper its smooth running. For example, testing of ATM switch.
- *Table-top testing* - Discussing business recovery arrangements using example of disasters.
- *Technical recovery testing* - Ensuring information systems can be restored effectively.
- *Testing recovery at an alternate site* - Running business processes in parallel with recovery operations away from the main site.
- *Tests of supplier facilities and services* – To ensure that externally provided services and products will meet the contracted commitment.
- *Complete rehearsals* - Testing that the organisation, personnel, equipment, facilities and processes can cope with interruptions.

Each organisation must define frequency, schedule and clusters of business areas selected for testing, after a thorough Risk and Business Impact Analysis has been done.

The bank can consider broad guidelines provided below for determining the testing frequency based on criticality of a process:

Processes	**Impact on processes**	**Table-top testing**	**Simulation testing**	**Component testing**	**Complete Rehearsals**
Process 1	High	Quarterly	Quarterly	Quarterly	Annually
Process 2	Medium	Quarterly	Half-yearly	Annually	Annually
Process 3	Low	Half-yearly	NA	NA	NA

9.2 Review /feedback of the BCP

BCPs should be reviewed and updated on the basis of the audit comments and the feedback received from different departments to ensure inclusion of such changes and the improvement. BCP procedures should be included within the organisation's management programme to ensure that business continuity matters are appropriately addressed. The periodicity may be decided by the bank itself.

Changes should follow the bank's formal management process which is in place for its policy or procedure documents. This formal change control process should ensure that the updated plans are distributed and reinforced by regular reviews of the complete plan.

10. Procedural aspects of BCP

a. BCP should take into account the potential of wide area disasters, which impact an entire region, and for resulting loss or inaccessibility of staff. It should also consider and address interdependencies, among various service providers.
b. In case the bank has implemented the CBS, they should consider running some critical processes and business operations from secondary sites or DR sites wherein each would provide back-up to the other. All critical processes should be documented to reduce dependency on personnel for scenarios where the staff is not able to reach the designated office premises.
c. Backup/standby personnel should be identified for all critical roles. A call matrix should be developed to better co-ordinate future emergency calls involving individual financial authorities, financial sector trade associations, and other banks and stakeholders.
d. Banks should consider having a detailed BCP for encountering natural calamity/disaster situation. A formal exception policy should be documented which will guide the affected areas' personnel to act independently till connection to the outside world is resumed.

11. Infrastructural Aspects of BCP

a. Banks should consider paying special attention to availability of basic amenities such as electricity, water and first-aid box in all offices.
b. In-house telecommunications systems and wireless transmitters on buildings should have backup power. Redundant systems, such as analogue line phones and satellite phones (where appropriate), and other simple measures, such as ensuring the availability of extra batteries for mobile phones, may prove essential to maintaining communications in case of a widescale infrastructure failure.
c. Banks should consider not storing critical papers, files, servers in the ground floors where there is possibility of floods or water logging. However, banks should also consider avoiding top floors in taller buildings to reduce impact due to probable fire.
d. Fire-proof and water-proof storage areas must be considered for critical documents.

e. Banks should consider having alternative means of power source (like procurement of more diesel/ emergency battery backup, etc.) for extended period of power cuts.
f. Banks should consider having an emergency helpline number or nationalised IVR message to resolve queries of customers and ensure that panic situation is avoided.

12. Human Resources Aspects of BCP

a. The bank should take into account the HR related issues which may arise while drafting the BCP. HR should, therefore, be an integral part in preparation of BCP. Generally, plans are often too focused on the technical issues. A separate section relating to people should be incorporated, including details on staff welfare, counselling, relocation considerations, etc.
b. BCP awareness programmes should also be implemented through induction programme newsletters, staff training exercises, etc., which serve to strengthen staff involvement in BCP.
c. Banks must consider training more than one individual staff for specific critical jobs (i.e., in the absence on one employee, the work must not be stalled or delayed). They must consider cross-training employees for critical functions and document-operating procedures.

13. Technology Aspects of BCP

There are many applications and services in banking system that are highly critical in nature and therefore requires high availability and fault tolerance to be considered while designing and implementing the solution. This aspect is to be taken into account especially while designing the data centre solution and the corporate network solution. One of the aspects of BCP related to technology is Disaster Recovery Planning.

13.1 Disaster Recovery

Prior to selecting a data recovery (DR) strategy, a DR planner should refer to their organisation's BCP, which should indicate key metrics of RPO and RTO for business processes.

Once, RTO and RPO metrics have been mapped to the IT infrastructure, the DR planner can determine the most suitable recovery strategy for each system. RTO and RPO metrics need to fit with the available budget and the criticality of the business process/function.

A disaster recovery plan is a part of the BCP. It must be a living document; any change in the functioning of the data centre, the plan must be updated to reflect those changes. It dictates every facet of the recovery process, including:

a. What events denote possible disasters.

b. What people in the organisation have the authority to declare a disaster and thereby put the plan into effect.
c. The sequence of events necessary to prepare the backup site once a disaster has been declared.
d. The roles and responsibilities of all key personnel with respect to carrying out the plan.
e. An inventory of the necessary hardware and software required to restore production.
f. A schedule listing the personnel that will be staffing the backup site, including a rotation schedule to support ongoing operations without burning out the disaster team members.

Generally, banks follow Core Banking Solution (CBS) for data recovery. Under CBS, the branches are linked to a centralised database at DC and all the functions are handled from a central server. In many cases, an organisation may elect to use an outsourced disaster recovery service provider to provide a stand-by site and systems rather than using their own remote facilities. In addition to preparing for the need to recover systems, organisations must also implement precautionary measures with an objective of preventing a disaster in the first place. These may include some of the following:

i. Uninterrupted power supply (UPS) or backup generator to keep systems going in the event of a power failure
ii. Fire preventions—alarms, fire extinguishers
iii. Anti-virus software and security measures

13.1.1 Backup site and implementing DR solution*:*

Backup site: Backup site is a location where an organisation can easily relocate following a disaster, such as fire, flood, terrorist threat or other disruptive event. This is an integral part of the disaster recovery plan and wider BCP of an organisation.

Types of backup sites

- Hot sites
- Cold sites
- Warm sites

Hot Sites: A hot site is a duplicate of the original site of the organisation, with full computer systems as well as near-complete backups of user data. Real-time synchronisation between the two sites may be used to mirror the data environment of the original site, using wide area network links and specialised software. Following a disruption to the original site, the hot site exists so that the organisation can relocate with minimal losses to normal operations.

Cold Sites: A cold site is the most inexpensive type of backup site for an organisation to operate. It does not include backed up copies of data and information from the original location of the organisation, nor does it include hardware already set up. The lack of hardware contributes to the minimal start-up costs of the cold site but requires additional time following the disaster to have the operation running at a capacity close to that prior to the disaster.

Warm Sites: A warm site is a compromise between hot and cold. These sites have hardware and connectivity already established, though on a smaller scale than the original production site or even a hot site. Warm sites have backups on hand, but they may not be complete and may be between several days and a week old. An example would be backup tapes sent to the warm site by courier.

Note: The major differences between them are determined by costs and effort required implementing each and on the architecture of the solution of the vendors.

13.1.2 Issues arising in implementing a DC/ DR solution in CBS

a. Solution architectures of DC and DR are not identical for all the applications and services provided by the vendors. Banks will have to conduct periodical review and upgrade the DR solutions from time to time and ensure that all the critical applications and services have a perfect replica in terms of performance and availability.
b. The configurations of servers, network devices and other products at the DC and DR have to be identical at all times. This includes the patches that are applied at the DC periodically and the changes made to the software from time to time by customisation and parameterisation to account for the regulatory requirements, system changes, etc.
c. Periodic checks with reference to ensuring data and transaction integrity between DC and DR are mandatory. Solutions have to have a defined RTO and RPO parameter. These parameters have a very clear bearing on the technology aspects as well as the process defined for cut over to the DR and the competency levels required moving over in the specified timeframe.
d. DR drills should be conducted periodically to see whether the DR is working or not. The support infrastructure at the DC and DR, viz., the electrical systems, air-conditioning environment and other support systems have no single point of failure and do have a building management and monitoring system to monitor the resources constantly and continuously.
e. Data replication mechanism followed between DC and DR is the asynchronous replication mechanism and implemented across the industry, either using database replication techniques or the storage-based replication techniques. The RPO is directly related to the latency permissible for the transaction data from the DC to update the database at the DR. Therefore, the process implemented for the data replication requirement must conform to the above and with no compromise to data and transaction integrity.

13.1.3 Issues/Challenges/Solutions in DC/DR implementation by Banks

a. Despite considerable advances in equipment and telecommunications design and recovery services, IT disaster recovery is becoming challenging. Continuity and recovery aspects are impacting IT strategy and cost implications are challenging IT budgets.
b. The time window for recovery is shrinking in face of the demand for 24 / 365 operations. This means that traditional off-site backup and restore methods are

often no longer adequate. It simply takes too long to recover incremental and full image backups of various inter-related applications (backed up at different times), synchronise them and re-create the position nearest to the disaster point. Continuous operation–data mirroring to offsite locations and standby computing and telecommunications–may be the only solution.

c. A risk assessment and business impact analysis should establish the justification for continuity for specific IT and telecommunication services and applications.

d. Achieving robust security (security assurance) is not a onetime activity. It is a continuous process that requires regular assessment of the security health of the organisation and proactive steps to detect and fix any vulnerability. Every bank should have in place quick and reliable access to expertise for tracking suspicious behaviour, monitoring users and performing forensics. Adequate reporting to the authorities concerned – such as the RBI/NABARD/ IDRBT/CERT-In and other institutions should be an automatic sub process whenever such events occur.

e. Telecommunications issues may also arise in the banks. It is important to ensure that relevant links are in place and that communications capability is compatible. The adequacy of voice and data capacity needs to be checked. Telephony needs to be switched from the disaster site to the standby site. A financial institution's BCP should consider addressing diversity guidelines for its telecommunications capabilities. Diversity guidelines should be considered by all financial institutions and should be commensurate with the institution's size, complexity, and overall risk profile. Diversity guidelines may include arrangements with multiple telecommunications providers. It is important for financial institutions to understand the relationship between their primary telecommunications carrier and various sub-carriers and how this complex network connects to their primary and back-up facilities.

f. Banks may consider the following telecommunications diversity components to enhance BCP:

    i. Alternative media, such as secure wireless systems
    ii. Internet protocol networking equipment that provides easily configurable rerouting and traffic load balancing capabilities
    iii. Local services to more than one telecommunications carrier's central office, or diverse physical paths to independent central offices
    iv. Separate power sources and separate connections to back up locations
    v. Regular use of multiple facilities in which traffic is continually split between the connections
    vi. Separate suppliers for hardware and software infrastructure needs.

g. Banks need to monitor their service relationship with telecommunications providers to manage the inherent risks more effectively. In coordination with vendors, management should ensure that risk management strategies include the following, at a minimum:

    i. Establish service level agreements that address contingency measures and change management for services provided
    ii. Ensure that primary and back-up telecommunications paths do not share a single point of failure
    iii. Establish processes to periodically inventory and validate telecommunications circuits and routing paths through comprehensive testing

h. *Outsourcing Risks* **-** Not every bank will be able to provide the DC/DR of its own due to various reasons. It is important to outsource all technology activities to a third-party service provider. A system integrator undertakes this activity who in turn outsource some of the activities to some other vendors but coordinates the activities as far as bank is concerned. It is the responsibility of the bank to ensure the activities are outsourced to those vendors, who apply the highest standards, having a stringent contract, clearly defining service specifications and technical requirements, and service-level agreements**.**

Annexure 1

Business Impact Analysis and Recovery Time Objectives (RTO)

Indicative scenario of various events. While preparing the BCP for the bank all such events should be put in plan and the time for recovery, responsibility, etc. should be mentioned.

Sr. No.	Events	Extent of Disruption	Recovery Time Objective (RTO)	Departments Concerned	Contact Officials
1	**Human Related Interruptions**				
1a	Strike by employees	• Whole Bank			
1b	Technology- not following security procedures.	• At Branches, Administrative offices, data centre, etc.			
2	**Equipment Breakdowns**	• Branches • administrative offices • data centre • network infrastructure • others			
3	**Environment related Interruptions**				
3a	Earthquake	• Cluster of branches • Administrative offices • data centre • networking, etc.		`	
3b	Flood	• Cluster of branches • administrative offices • data centre, etc.			
3c	Major Fire / Bombing	• At Branches • Administrative offices • data centre, etc.			
3d	Effluent / Gas Leakage	• Cluster of branches • Administrative offices • data centre • networking ,etc.			

Annexure 2

Sample incidents and suggested actions while preparing BCP

Incident	Extent of disruption	Suggested Action to be taken
Power failure	Affected places	Switch on the UPS. Start the generator set.
Failure of electricity supply	Affected places	UPS will draw power from batteries first and from generators beyond five minutes, automatically. Follow up action to be initiated for restoration of power. Simultaneously, non-critical and unnecessary systems must be switched off so that the power could be made available to critical systems for more time.
Failure of one UPS system	Affected places	It is advisable to keep two units of UPS and split the supply of current to the computers through segmented approach, by connecting one server with one UPS and the other server with other UPS so as to build redundancy in the system.
Draining of batteries coupled with failure of raw power	Affected places	Since both raw power and power from batteries will not be available, system administrator has to start the generator. Proactive action shall also be taken by getting the functioning of batteries at regular periodical intervals. Simultaneously, system administrator should obtain vendor support for replacement of batteries.
Air-conditioners not working	No effect	System administrator through Administration Section should notice the failure of AC units, obtain vendor support for setting right the problem.

Annexure 3
Sample incidents of hardware failures and suggested action

Incident	Effect	Action
Internet banking server is not working	No access to internet banking	System administrator should obtain vendor support for setting right the problem.
Ethernet card fails	System halts	The system administrator should take vendor support for physically shifting the connectivity to the second ethernet card so that the system can be brought to up and working status.
Routers are not working	Network connectivity	System administrator should obtain vendor support for setting right the problem.
Security systems not functioning	System halts	System administrator should obtain vendor support for setting right the problem.

Annexure 4

Sample incidents of software failures and suggested action

Incident	Effect	Action
Operating system problems	System halts	System administrator should obtain vendor support for setting right the problem
Database related problems	System halts	System administrator should obtain vendor support for setting right the problem
Core Banking Solutions related problems	System halts	System administrator should obtain vendor support for setting right the problem
Application software (internet banking) related problems	System halts	System administrator should obtain vendor support for setting right the problem
Data corruption	System halts	System administrator should restore the data from the latest back-up
Back-up not retrievable	System halts for one hour	System administrator should reconstruct the earlier backup with the help of logs.

Annexure 5

Sample Incidents of network failure and suggested action

Incident	Effect	Action
Leased line link for internet banking fails	No effect	The system automatically triggers the ISDN link. However, the system administrator has to obtain the vendor support to bring the leased line link up and working at the earliest.
Both leased line and ISDN links fail	System halts	The system administrator has to obtain the vendor support to bring the links up and working
Router fails	System halts	The system administrator has to obtain the vendor support to set right the problem, if necessary, by organising a standby router.
Port failure at ISP end	System halts for a short time	The system administrator has to obtain the vendor support to change the port settings.
Modem failures	System halts for a short time	The system administrator has to obtain the vendor support to shift over to a standby modem

Other failures

Incident	Effect	Action
Virus attack	System slows down/ halts	The system administrator has to obtain the vendor support to set right the problem
Denial of service attacks	System slows down/ halts	The system administrator has to obtain the vendor support to set right the problem

Annexure 6

Indicative checklist of security precaution at branches

1. Are minimum two staff members present while opening the branch?
2. If armed guard is posted, is he normally present while opening the branch?
3. As and when individual staff members enter the branch are the gates closed and locked again?
4. Are the channel gates kept half opened and chained during business hours?
5. At the close of banking hours, is the collapsible/grill gate kept locked and entry to genuine customers/visitors allowed only on identification and after taking clearance from the Branch Manager?
6. Is the armed guard, wherever posted, deployed in a suitable place so that he can have full view of the banking hall and use his weapon effectively against the criminals?
7. Is the armed guard utilised only on security duties?
8. Is entry of customers/visitors inside staff working area monitored and controlled?
9. Is the fire extinguisher refilled in time/checked?
10. Is the alarm system tamperproof, wherever provided?
11. Is the alarm system in working condition and kept always in 'ON' position?
12. Are the staff familiar with the operation of alarm system and location of its switches?
13. Are the cash holding limits adhered to?
14. Are important telephone numbers prominently displayed?
15. Are important telephone numbers kept in personal diary of the Branch Manager/ Accountant?
16. Do the windows/ventilators have strong grills?
17. Are the cash cabins kept locked from inside during business hours?
18. Are the antecedents of owners and drivers checked before selecting vehicles for cash remittance?
19. Is there periodical checking/maintenance of all electrical equipments like transformers, switchboards, air conditioners and computers?
20. Are circuit breakers used in electrical circuits?
21. Are backup documents kept at safer premises, off-site?
22. Are the fire extinguishers serviced periodically?
23. Are the staffs trained in use of fire extinguishers?
24. Is the premises kept clean?
25. Are stationery items kept properly stacked in racks?
26. Are the branches/offices a 'No Smoking' area?
27. Are waster papers kept in receptacles and are they disposed off properly and regularly?

Annexure 7

Emergency Service Listings

Branch	Service	Contact Nos.
Police Stations	City Control Room	**100**
	Police Head Quarter	
	Traffic Police	
	Police Station 1	
	Police Station 2	
Fire Department	City Control Room	
	Fire Station 1	
	Fire Station 2	
District Administration	Commissioner	
	Collector	
	Superintendent of Police	
Hospitals / Ambulance Service	Hospital 1	
	Hospital 2	
	Hospital 3	
	Hospital 4	
Important Contacts of Service providers	Lawyers	
	Valuers	
	Electrician	
	Plumber	
	Carpenter	