Chapter 7: Business Continuity Planning

Introduction

The pivotal role that banking sector plays in the economic growth and stability, both at national and individual level, requires continuous and reliable services. Increased contribution of 24x7 electronic banking channels has increased the demand to formulate consolidated Business Continuity Planning (BCP) guidelines covering critical aspects of people, process and technology.

BCP forms a part of an organisation's overall Business Continuity Management (BCM) plan, which is the "preparedness of an organisation", which includes policies, standards and procedures to ensure continuity, resumption and recovery of critical business processes, at an agreed level and limit the impact of the disaster on people, processes and infrastructure (includes IT); or to minimise the operational, financial, legal, reputational and other material consequences arising from such a disaster.

Effective business continuity management typically incorporates business impact analyses, recovery strategies and business continuity plans, as well as a governance programme covering a testing programme, training and awareness programme, communication and crisis management programme.

1. Roles, Responsibilities and Organisational structure

Board of Directors and Senior management

A bank's Board has the ultimate responsibility and oversight over BCP activity of a bank. The Board approves the Business Continuity Policy of a bank. Senior Management is responsible for overseeing the BCP process which includes*:*

- Determining how the institution will manage and control identified risks
- Allocating knowledgeable personnel and sufficient financial resources to implement the BCP
- Prioritizing critical business functions
- Designating a BCP committee who will be responsible for the Business Continuity Management
- 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.
- The top management should consider evaluating the adequacy of contingency planning and their periodic testing by service providers whenever critical operations are outsourced.
- Ensuring that the BCP is independently reviewed and approved at least annually;
- Ensuring employees are trained and aware of their roles in the implementation of the BCP
- Ensuring the BCP is regularly tested on an enterprise-wide basis
- Reviewing the BCP testing programme and test results on a regular basis and
- Ensuring the BCP is continually updated to reflect the current operating environment

1.1 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:

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

1.2 BCP Committee or Crisis Management Team

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 has to be prepared for a recovery process, aimed at protection of critical functions. To this end, it would be helpful if a set up like the BCP Committee, charged with the implementation of BCP, in an eventuality and all departments expected to fulfill their respective roles in a co-ordinated manner.

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

- To exercise, maintain and to invoke business continuity plan, as needed
- Communicate, train and promote awareness
- Ensure that the Business Continuity Plan (BCP) fits with other plans and requirement of concerned authorities
- Budgetary issues
- Ensure training and awareness on BCP to concerned teams and employees
- Co-ordinating the activities of other recovery, continuity, response teams and handling key decision-making
- They determine the activation of the BCP
- Other functions entail handling legal matters evolving from the disaster, and handling public relations and media inquiries

1.3 BCP 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 organizing 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 contractors 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:	**Spokesperson (Communications)**
Topic	Ideas
1. Roles, responsibilities and authorities	CEO- Spokesperson PR and marketing Designated senior official Internal and external communications
2. Necessary	Media training

competencies	Write coherent briefs Be up-to-date with mission statement, value statement and general company policies Consistency with message
3. Approach to training needs analysis	Identify gaps in knowledge and liaise with appropriate departments, whose message will be included(e.g. Health and Safety)
4. Appropriate training	Exercises
5. Ways of measuring necessary competence	Review Notes
6. Suitable records of education, training, skills, experience and qualifications	Past exercise reports

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. Ways of measuring necessary competence	Through exercising Predefine success criteria and review Measure plan and people Range of exercise types • Desktop • Simulation
6. Suitable records of education, training, skills, experience and qualifications	Records of training participation • Memberships • Formal qualifications • Personal development plans

2. Critical Components of Business Continuity Management Framework

The BCP requirements enunciated in this document should be considered. The onus lies on the Board and Senior Management for generating detailed components of BCP in the light of an individual bank's activities, systems and processes.

2.1 BCP Methodology

Banks should consider looking at BCP methodologies and standards–BS 25999 by BSI– which follows the "Plan-Do-Check-Act Principle".

BCP methodology should include:

Phase 1: Business Impact Analysis

- Identification of critical businesses, owned and shared resources with supporting functions to come up with the Business Impact Analysis (BIA)
- Formulating Recovery Time Objectives (RTO), based on BIA. It may also be periodically fine-tuned by benchmarking against industry best practices
- Critical and tough assumptions in terms of disaster, so that the framework would be exhaustive enough to address most stressful situations
- Identification of the Recovery Point Objective (RPO), for data loss for each of the critical systems and strategy to deal with such data loss
- Alternate procedures during the time systems are not available and estimating resource requirements

Phase 2: Risk Assessment

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

iii) Impact on restoring critical business functions, including customer-facing systems and payment and settlement systems such as cash disbursements, ATMs, internet banking, or call centres

- Dependency and risk involved in use of external resources and support

Phase 3: Determining Choices and Business Continuity Strategy

- BCP should evolve beyond the information technology realm and must also cover people, processes and infrastructure
- The methodology should prove for the safety and well-being of people in the branch / outside location at the time of the disaster.
- Define response actions based on identified classes of disaster.
- 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

- Action plans, i.e.: defined response actions specific to the bank's processes , practical manuals(do and don'ts, specific paragraph's customised to individual business units) and testing procedures
- Establishing management succession and emergency powers
- Compatibility and co-ordination of contingency plans at both the bank and its service providers
- The recovery procedure should not compromise on the control environment at the recovery location
- Having specific contingency plans for each outsourcing arrangement based on the degree of materiality of the outsourced activity to the bank's business
- 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)

2.3 Key Factors to be Considered for BCP Design

Following factors should be considered while designing the BCP:

- Probability of unplanned events, including natural or man-made disasters, earthquakes, fire, hurricanes or bio-chemical disaster
- Security threats
- Increasing infrastructure and application interdependencies
- Regulatory and compliance requirements, which are growing increasingly complex
- Failure of key third party arrangements
- Globalisation and the challenges of operating in multiple countries.

2.4 BCP Considerations

(a) Banks must consider implementing a BCP process to reduce the impact of disruption, caused by disasters and security failures to an acceptable level through a combination of preventive and recovery measures.
(b) BCP should include measures to identify and reduce probability of risk to limit the consequences of damaging incidents and enable the timely resumption of essential operations. BCP should amongst others, consider reputation, operational, financial, regulatory risks.
(c) The failure of critical systems or the interruption of vital business processes could prevent timely recovery of operations. Therefore, financial institution management must fully understand the vulnerabilities associated with interrelationships between various systems, departments, and business processes. These vulnerabilities should be incorporated into the BIA, which analyses the correlation between system components and the services they provide.
(d) Various tools can be used to analyse these critical interdependencies, such as a work flow analysis, an organisational chart, a network topology, and inventory records. A work flow analysis can be performed by observing daily operations and interviewing employees to determine what resources and services are shared among various departments. This analysis, in conjunction with the other tools, will allow management to understand various processing priorities, documentation requirements, and the interrelationships between various systems. The following issues when determining critical interdependencies within the organisation:
    i. Key personnel;
    ii. Vital records;
    iii. Shared equipment, hardware, software, data files, and workspace;
    iv. Production processes;
    v. Customer services;
    vi. Network connectivity; and
    vii. Management information systems.

(e) Key Considerations while Formulating A BCP:
- Ensuring prompt and accurate processing of securities transactions, including, but not limited to, order taking, order entry, execution, comparison, allocation, clearance and settlement of securities transactions, the maintenance of customer accounts, access to customer accounts and the delivery of funds and securities.
- Honouring of all customer payouts (i.e. obligation)
- Providing priority to intra-day deal payment
- Providing customers prompt access to their funds and securities – measures should be undertaken to make customer funds and securities available to customers in the event of a significant business disruption.
- Continuing compliance with regulatory reporting requirements etc.

(f) A single framework of BCP should be maintained to ensure that all plans are consistent, and to identify priorities and dependencies for testing and maintenance.

A BCP framework should consider the following:

- Conditions for activating plans, which describe aprocess to be followed (how to assess the situation, who is to be involved, etc.) before each plan is activated
- Emergency procedures, which describe the actions to be taken following an incident which jeopardises business operations and/ or human life. This should include arrangements for public relations management and for effective liaison with appropriate public authorities e.g. police, fire service, health-care services and local

government

- Identification of the processing resources and locations, available to replace those supporting critical activities; fall back procedures which describe the actions to be taken to move essential business activities or support services to alternative temporary locations and to bring business processes back into operation in the required time-scales
- Identification of information to be backed up and the location for storage, as well as the requirement for the information to be saved for back-up purpose on a stated schedule and compliance therewith
- Resumption procedures, which describe the actions to be taken to return to normal business operations
- A maintenance schedule which specifies how and when the plan will be tested and the process for maintaining the plan
- Awareness and education activities, which are designed to create understanding of critical banking operations and functions, business continuity processes and ensure that the processes continue to be effective
- The responsibilities of the individuals, describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.

(g) Pandemic Planning

Pandemics are defined as epidemics, or outbreaks in humans, of infectious diseases that have the ability to spread rapidly over large areas, possibly worldwide. Adverse economic effects of a pandemic could be significant, both nationally and internationally. Due to their crucial financial and economic role, financial institutions should have plans in place that describe how they will manage through a pandemic event.

Pandemic planning presents unique challenges to financial institution management. Unlike natural disasters, technical disasters, malicious acts, or terrorist events, the impact of a pandemic is much more difficult to determine because of the anticipated difference in scale and duration. Further, while traditional disasters and disruptions normally have limited time durations, pandemics generally occur in multiple waves, each lasting two to three months. Consequently, no individual or organisation is safe from the adverse effects that might result from a pandemic event.

One of the most significant challenges likely from a severe pandemic event will be staffing shortages due to absenteeism. These differences and challenges highlight the need for all financial institutions, no matter their size, to plan for a pandemic event when developing their BCP.

It is important for institutions to actively keep abreast of international and national developments and health advisories issued in this regard.

Accordingly, a bank's BCP needs to provide for the following:

1. A preventive programme to reduce the likelihood that a bank's operations will be significantly affected by a pandemic event, including: monitoring of potential outbreaks, educating employees, communicating and coordinating with critical service providers and suppliers, in addition to providing appropriate hygiene training and tools to employees.

2. A documented strategy that provides for scaling the institution's pandemic efforts so they are consistent with the effects of a particular stage of a pandemic outbreak, such as first cases of humans contracting the disease overseas or in India and first cases within the organisation itself. The strategy will also need to outline plans that

state how to recover from a pandemic wave and proper preparations for any following wave(s).

3. A comprehensive framework of facilities, systems, or procedures that provide the organisation the capability to continue its critical operations in the event that large numbers of the institution's staff are unavailable for prolonged periods. Such procedures could include social distancing to minimise staff contact, telecommuting, redirecting customers from branch to electronic banking services, or conducting operations from alternative sites.

4. The framework should consider the impact of customer reactions and the potential demand for, and increased reliance on, online banking, telephone banking, ATMs, and call support services. In addition, consideration should be given to possible actions by public health and other government authorities that may affect critical business functions of a financial institution.

5. A testing programme to ensure that the institution's pandemic planning practices and capabilities are effective and will allow critical operations to continue.

6. An oversight programme to ensure ongoing review and updates to the pandemic plan so that policies, standards, and procedures include up-to-date, relevant information provided by governmental sources or by the institution's monitoring programme.

3. Testing A BCP

– *Banks must regularly test BCP to ensure that they are up to date and effective:* Testing of BCP should include all aspects and constituents of a bank i.e. people, processes and resources (including technology). BCP, after full or partial testing may fail. Reasons are incorrect assumptions, oversights or changes in equipment or personnel. 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. It is recommended to test the individual components of the plans(s) frequently, typically at a minimum of once a year. A variety of techniques should be used in order to provide assurance that the plan(s) will operate in real life.

– *Banks should involve their Internal Auditors (including IS Auditors) to audit the effectiveness of BCP:* And its periodic testing as part of their Internal Audit work and their findings/ recommendations in this regard should be incorporated in their report to the Board of Directors.

– *Banks should consider having a BCP drill planned along with the critical third parties:* In order to provide services and support to continue with pre-identified minimal required processes.

– *Banks should also periodically moving their operations:* Including people, processes and resources (IT and non-IT) to the planned fall-over or DR site in order to test the BCP effectiveness and also gauge the recovery time needed to bring operations to normal functioning.

– *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.

– *Banks should consider having unplanned BCP drill:* Wherein only a restricted set of people and certain identified personnel may be aware of the drill and not the floor or business personnel. In such cases banks should have a "Lookout Team" deployed at the location to

study and assimilate the responses and needs of different teams. Based on the outcome of this study, banks should revise their BCP Plan to suit the ground requirements.

3.1 Testing Techniques

The below are few of the illustrative techniques that can be used for BCP testing purposes:

- **Table-top testing** for scenarios (discussing business recovery arrangements using example interruptions)
- **Simulations** (particularly for training people in their post-incident or crisis management roles)
- **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** (ensuring 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)

a) Simulation testing: It is when participants choose a specific scenario and simulate an on-location BCP situation. It involves testing of all resources: 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. It can also specify role playing with simulated response at alternate locations/facilities to act out critical steps, recognise difficulties, and resolve problems.

b) 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.

Each organisation must define frequency, schedule and clusters of Business Areas, selected for test after a through Risk and Business Impact Analysis has been done.

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

Impact on processes	Table-top testing	Call tree	Simulation testing	Component testing	Complete Rehearsals
High	Quarterly	Quarterly	Quarterly	Quarterly	Annually
Medium	Quarterly	Half-yearly	Half-yearly	Annually	Annually
Low	Half-yearly	Annually	NA	NA	NA

4. Maintenance and Re-assessment of Plans

(a) BCPs should be maintained by annual reviews and updates to ensure their continued effectiveness. Procedures should be included within the organisation's change management programme to ensure that business continuity matters are appropriately addressed. Responsibility should be assigned for regular reviews of each business continuity plan. The identification of changes in business arrangements/processes, not yet reflected in the business continuity plans, should be followed by an appropriate update of the plan on a periodic basis, say quarterly. This would require a process of conveying any changes to the institution's business, structure, systems, software, hardware, personnel, or facilities to the BCP coordinator/team. If significant changes have occurred in the business environment, or if audit findings warrant changes to the BCP or test programme, the business continuity policy guidelines and programme requirements should be updated accordingly.

(b) Changes should follow the bank's formal change management process 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.

(c) A copy of the BCP, approved by the Board, should be forwarded for perusal to the RBI on an annual basis. In addition, the bank should also submit:

– An annual statement at the end of each financial year describing the critical systems, their Rots and the bank's strategy to achieve them, and

– A quarterly statement, reporting major failures during the period for critical systems, customer segment or services impacted due to the failures and steps taken to avoid such failures in future.

5. Procedural aspects of BCP

(a) An effective 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 inter dependencies, both market-based and geographic, among financial system participants as well as infrastructure service providers.

(b) Further, banks should also consider the need to put in place necessary backup sites for their critical payment systems which interact with the systems at the Data centres of the Reserve Bank.

(c) Banks may also consider running some critical processes and business operations from primary and the secondary sites, wherein each would provide back-up to the other.

(d) Namely prioritising process and alternative location for personnel in the following categories:

- Dealers and traders
- Operations (eh: teller, loan desk, cash desk etc.)
- Treasury department staff
- Sales staff
- IT staff
- Corporate functions (HR, Admin) staff

- Comprehensive testing would help banks to further fine-tune BCP/DR processes to ensure their robustness and also enable smooth switch-over to the DR site, as per the priority and scale of processes identified for each process.

(e) 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.

(f) 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. In addition the organisation should have calling tree with branches across specific region/business processes. Based on the nature of the emergency a particular branch/the entire calling tree should be activated.

(g) The relevant portion of the BCP adopted should also be disseminated to all concerned, including the customers, so that the awareness would enable them to react positively and in consonance with the BCP. This would help maintain the customer's faith on the banking institution, and the possibility of a bank-run would be exponentially minimised. The part of the plan kept in the public domain should normally be confined to information relating to the general readiness of the banks in this regard without any detailed specifics, to protect the banks from becoming vulnerable to security threats

(h) Banks should consider formulating a clear 'Communication Strategy' with the help of media management personnel to control the content and form of news being percolated to their customers in times of panic.

(i) Banks should consider having a detailed BCP plan 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.

(j) The above mentioned guideline should have exceptions documented for critical process which will ensure continuation of critical process without the regular operational formalities.

(k) After appropriate approvals or permissions are obtained, banks should consider having a guideline ready on relaxing certain rules/ requirements for customers affected by the calamity.

(l) Like:

- Extending loan/interest payment timeliness
- Issuance of fresh loan with minimal required documents
- Waving off late payment fees and penalties in certain cases
- Allowing more than normal cash withdrawal from ATM's

(m) Banks can consider expediting cheque clearing for customers by directing all cheques to a different region than the one affected by the calamity. In case of severe calamity banks should consider restricting existing loans to facilitate rebuilding efforts by the Govt. for the calamity areas. The banks may also be consider ensuring quick processing of loan applications, preferably within 48 hours of receipt of such applications. It should consider dispatching credit bill, agreement notes, etc. due to customer by having an arrangement to print the same at an alternative location and

should consider accepting late payments for credit card dues for customers in the calamity affected area.

(n) In the face of a natural disaster, RBI may also consider allowing banks to open temporary branches, under advice to it, by relaxing norms for opening of temporary branches, and stipulating that such branches should be closed within 30 days of opening. Banks should also endeavor for resumption of banking services by setting up satellite offices, extension counters or mobile banking facilities.

6. Infrastructure Aspects of BCP

– Banks should consider paying special attention to availability of basic amenities such as electricity, water and first-aid box in all offices. (erg. evaluate the need of electricity backup not just for its systems but also for its people and running the infrastructure like central air-conditioning.)

– Banks should consider assigning ownership for each area. Emergency procedures, manual fallback plans and resumption plans should be within the responsibility of the owners of the appropriate business resources or processes involved.

– 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 a wide-scale infrastructure failure.

– Possible fallback arrangements should be considered and alternative services should be carried out in co-ordination with the service providers, contractors, suppliers under written agreement or contract, setting out roles and responsibilities of each party, for meeting emergencies. Also, imposition of penalties, including legal action, may be initiated by an organisation against service providers or contractors or suppliers, in the event of noncompliance or non-co-operation.

– When new requirements are identified, established emergency procedures: erg. evacuation plans or any existing fallback arrangements, should be amended as appropriate.

– Banks may consider having backup resources (erg. stationery required for cheque printing, special printers, stamps) at a secondary operational location.

– The plans may also suitably be aligned with those of the local government authorities

– 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 building to reduce impact due to probable fire.

– Fire-proof and water-proof storage areas must be considered for critical documents.

– Banks should consider having alternative means of power source (like procurement of more diesel/ emergency battery backup etc.) for extended period of power cuts.

– Banks should consider having an emergency helpline number or nationalised IVR message to resolve queries of customers and ensure that panic situation is avoided. For this an alternative backup area call centre should be identified to take over part load of the calamity affected area. Designated person/ team must be responsible for enabling line diversion. A similar service can also be considered for the benefit of employee related communication.

7. Human Aspects of BCP

People are a vital component of any organisation. They should therefore be an integral part of a BCP. Generally, plans are often too focused on the technical issues, therefore, it is suggested that a separate section relating to people should be incorporated, including details on staff welfare, counseling, relocation considerations, etc. BCP awareness programmer should also be implemented which serve to strengthen staff involvement in BCP. This can be done through induction programme newsletters, staff training exercises, etc.

Banks must consider training more than one individual staff for specific critical jobs (ire. 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. Banks should consider possibility of enabling work-from--home capabilities and resources for employees performing critical functions.

Role of HR in the BCP context

a) Crisis Management Team: As a core member of the CMT, HR provides guidance to team on people-related issues, including evacuation, welfare, whether to invoke the HR incident line, alternative travel arrangements and what to communicate to staff.

b) HR Incident Line: Operated from within the centralised HR function, the incident helpline is invoked in those instances, where there are possible casualties or missing staff, as a result of an incident. Invoked by the CMT, the line is manned by qualified HR officers trained in how to deal with distressed callers. The staff may be provided with an emergency card, which includes the incident line number. Information on the hotline is updated on a regular basis. The facility enables line managers to keep the central crisis team up to speed on the whereabouts and well-being of staff. Ongoing welfare and support for staff is also provided via an employee assistance provider.

c) Exceptional Travel arrangements: Transportation plans should be considered in the event of the need to relocate. Key staff need to be identified including details of where they are located, and vehicles are on standby to transport them if required.

8. Technology Aspects of BCP

The are many applications and services in banking system that are highly mission 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.

Data Recovery Strategies

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

Recovery Point Objective (RPO)–The acceptable latency of data that will be recovered

Recovery Time Objective (RTO)–The acceptable amount of time to restore the function

Recovery Point Objective must ensure that the Maximum Tolerable Data Loss for each activity is not exceeded. The **Recovery Time Objective** must ensure that the Maximum Tolerable Period of Disruption (MTPD), for each activity, is not exceeded. The metrics specified for the business processes must then be mapped to the underlying IT systems and infrastructure that support those 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. An important note here, however, is that the business ultimately sets the IT budget. Therefore, RTO and RPO metrics need to fit with the available budget and the critical of the business process/function.

A List of Common Strategies for Data Protection:

- Backups made to tape and sent off-site at regular intervals (preferably daily)
- Backups made to disk on-site and automatically copied to off-site disk, or made directly to off-site disk
- Replication of data to an off-site location, which overcomes the need to restore the data (only the systems then need to be restored or synced). This generally makes use of storage area network (SAN) technology
- High availability systems that keep both data and system replicated, off-site, enabling continuous access to systems and data

In many cases, an organisation may elect to use an outsourced disaster recovery 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:*

- Local mirrors of systems or data. Use of disk protection technology such as RAID
- Surge protectors—to minimise the effect of power surges on delicate electronic equipment
- Uninterrupted power supply (UPS) or backup generator to keep systems going in the event of a power failure
- Fire preventions—alarms, fire extinguishers
- Anti-virus software and security measures

A disaster recovery plan is a part of the BCP. It dictates every facet of the recovery process, including:

- What events denote possible disasters;
- What people in the organisation have the authority to declare a disaster and thereby put the plan into effect;
- The sequence of events necessary to prepare the backup site once a disaster has been declared;
- The roles and responsibilities of all key personnel with respect to carrying out the plan;
- An inventory of the necessary hardware and software required to restore production;
- 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.

A disaster recovery plan must be a living document; as the data centre changes, the plan must be updated to reflect those changes.

It is to be noted that the technology issues are a derivative of the Business Continuity plan and Management.

For example, BCP and Management will lead to the Business Impact Analysis, which will lead to the Performance Impact Analysis (PIA). That will depend on the Technology Performance of the total IT Solution Architecture.

To amplify business impact analysis is to identify the critical operations and services, key internal and external dependencies and appropriate resilience levels. It also analysis the risks and quantify the impact of those risks from the point of view of the business disruptions. For example, in order to provide state of the art customer services both at the branch level and the delivery channels we need to take into account the services levels that are committed.

If an ATM transaction has to take place in 10 seconds and cash withdrawal or deposit has to take place in 60 seconds at the counter, then based on the load one can compute the number of customers who can be serviced in a day. The above example is to understand the fact that the business latency introduced by the system is a combination of technology, process and people. Therefore, the technical latency is a derivative of the committed business latency and the technology solution architecture has to deliver the same under varying loads.

Technology Solution Architecture to address specific BCM requirements are:

- Performance
- Availability
- Security and Access Control
- Conformance to standards to ensure Interoperability

Performance of the technology solution architecture for operations needs to be quantified. It should be possible to measure, as and when required, the quantified parameters. (For example, if the latency for a complex transaction initiated at the branch has to be completed in four seconds under peak load, it should be possible to have adequate measuring environments to ensure that performance degradations have not taken place due to increasing loads.)

Solution architecture has to be designed with high-availability, and no single point of failure. It is inevitable that a complex solution architecture with point products from different sources procured and implemented at different points in time will have some outage once in a while and the important issue is that with clearly defined SLAs, mean time to restore, it should be possible to identify the fault and correct the same without any degradation in performance.

Accordingly, with respect to the performance and availability aspects the following architectures have to be designed and configured to provide high levels of up time round the clock to ensure uninterrupted functioning.

Summation of the required processes:

–Data centre solution architecture

–DR solution architecture

–Near site solution architecture

–Enterprise network and security architecture

– Branch or delivery channel architecture

– *Based on the above observation, banks are required to do the following:* Take up the performance and availability audit of the solutions deployed to ensure that the architecture is designed and implemented with no single point of failure.

– Audit the deployed architecture for all the mission critical applications and services and resolve the concerns that arise in a time bound manner.

– Periodically investigate the outages that are experienced from time to time, which are mini disasters that result in non availability of services for a short span of time, systems not responding when transactions are initiated at the branch level, delivery channels not functioning for a brief period of time to ensure that the customer service is not affected.

– Ensure availability of appropriate technology solutions to measure and monitor the functioning of products. And, have competent and capable technical people within the system to resolve issues expeditiously. (*Issues relating to manpower training needs are further elaborated at Annex-B*)

The issues detailed above have to be borne in mind while finalising the data centre architecture and the corporate network architecture which are expected to have redundancy built in the solution with no single point of failure.

With reference to the network architecture it is recommended that the Banks built in redundancies as under:

- Link level redundancy
- Path level redundancy
- Route level redundancy
- Equipment level redundancy
- Service provider level redundancy

Issues in choosing a backup site and implementing a DC or DR solution:

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 business continuity planning of an organisation. A backup site can be another location operated by the organisation, or contracted via a company that specialises in disaster recovery services. In some cases, an organisation will have an agreement with a second organisation to operate a joint backup site.

There are three main types of backup sites:

- *cold sites*
- *warm sites*
- *hot sites*

Differences between them are determined by costs and effort required to implement each. Another term used to describe a backup site is a work area recovery site.

1. 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.

2. 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. Ideally, a hot site will be up and running within a matter of hours or even less. Personnel may still have to be moved to the hot site so it is possible that the hot site may be operational from a data processing perspective before staff has relocated. The capacity of the hot site may or may not match the capacity of the original site depending on the organisation's requirements. This type of backup site is the most expensive to operate. Hot sites are popular with organisations that operate real time processes such as financial institutions, government agencies and ecommerce providers

3. Warm Sites: A warm site is, quite logically, a compromise between hot and cold. These sites will have hardware and connectivity already established, though on a smaller scale than the original production site or even a hot site. Warm sites will 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.

8.1 The following issues arise in choosing a back up site and implementing a DC/DR solution*:*

1. Solution architectures of DC and DR are not identical for all the applications and services. Critical applications and services, namely the retail, corporate, trade finance and government business solutions as well as the delivery channels are having the same DR configurations whereas surround or interfacing applications do not have the DR support. Banks will have to conduct periodical review with reference to the above aspect 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.

2. 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 customization and parameterization to account for the regulatory requirements, system changes etc .

3. Periodic checks with reference to ensuring data and transaction integrity between DC and DR are mandatory. It could be done over the week end or as a part of the EoD / BoD process.

4. Solutions have to have a defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) parameter. These two 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 to move over in the specified time frame.

5. Values chosen for the RTO and RPO is more to follow the industry practice and not derived from first principles. Therefore, the DR drills that are conducted periodically have to ensure that the above parameters are strictly complied with.

6. Technology operations processes which support business operations (such as EOD/ BOD) need to formally included into the IT Continuity Plan.

7. Banks may also consider Recovery Time Objective and Recovery Point Objectives (RTO/ RPO) for services being offered and not just a specific application. For example--for internet

portal and not retail banking. This is done to avoid any inconsistency in business users understanding.

6. DR drills currently conducted periodically come under the category of planned shutdown. Banks have to evolve a suitable methodology to conduct the drills which are closer to the real disaster scenario so that the confidence levels of the technical team taking up this exercise is built to address the requirement in the event of a real disaster.

7. It is also recommended that the support infrastructure at the DC and DR, namely 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 constantly and continuously monitor the resources. If it is specified that the solution has a high availability of 99.95 measured on a monthly basis and a mean time to restore of 2 hrs in the event of any failure, it has to include the support system also.

8. 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. They do have relative merits and demerits. The RTO and RPO discussed earlier, along with the replication mechanism used and the data transfer required to be accomplished during the peak load will decide the bandwidth required between the DC and the DR. 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 has to conform to the above and with no compromise to data and transaction integrity.

9. Given the need for drastically minimizing the data loss during exigencies and enable quick recovery and continuity of critical business operations, banks may need to consider near site DR architecture. Major banks with significant customer delivery channel usage and significant participation in financial markets/payment and settlement systems may need to have a plan of action for creating a near site DR architecture over the medium term (say, within three years).

To address these issues, RBI may consider:

- Stipulating a periodic DR exercise with clearly defined ground rules for the same. IT recovery tests are also required to realistically reflect the worst case scenario where all critical systems must be restored concurrently.
- Sending out detailed questionnaires to the banks based on the questionnaire that is issued by CPSS-IOSCO.
- Carrying out system wide stress testing simulating various scenarios, elaborated in the next section.

8.2 Issues/Challenges in DC/DR implementation by the 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. Some studies claim that around 30 percent of high-availability applications have to be recovered in less than three hours. A further 45 percent within 24 hours, before losses become unsustainable; others claim that 60 percent of Enterprise Resource Planning (ERP) Systems have to be restored in under 24 hours. 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 as at disaster. Continuous operation–data mirroring to off-site 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 cannot be obtained just by purchasing and installing suitable software and hardware. 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 behavior, monitoring users and performing forensics. Adequate reporting to the authorities concerned – such as the RBI/ IDRBT/CERT-In and other institutions should be an automatic sub process whenever such events occur.

Important steps that need to be institutionalised are the following:

a) Rigorous self-assessment of security measures by banks and comprehensive security audit by external agencies, as detailed under the “Chapter on Information Security” earlier.

b) Random Security Preparedness. It is proposed that a sufficiently large ``question bank'' related to security health of the organization be prepared and given to RBI's inspection teams who go for inspection of banks. A random subset of these queries could then be given to a bank’s IT team for which answers need to be provided in near real time. Sample checks related to user accounts could be the number of new accounts, terminated accounts, most active accounts. There could also be demonstrations of data recovery from archives.

(e) **Telecommunications issues may also arise: I**t 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. This is particularly important for the financial services sector that provides critical payment, clearing, and settlement processes; however, 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. However, diverse routing may be difficult to achieve since primary telecommunications carriers may have an agreement with the same sub-carriers to provide local access service, and these sub-carriers may also have a contract with the same local access service providers. Financial institutions do not have any control over the number of circuit segments that will be needed, and they typically do not have a business relationship with any of the sub-carriers. Consequently, it is important for financial institutions to understand the relationship between their primary telecommunications carrier and these various sub-carriers and how this complex network connects to their primary and back-up facilities. To determine whether telecommunications providers use the same sub-carrier or local access service provider, banks may consider performing an end-to-end trace of all critical or sensitive circuits to search for single points of failure such as a common switch, router, PBX, or central telephone office.

(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 re-routing 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) Multiple, geographically diverse cables and separate points of entry

(v) Frame relay circuits that do not require network interconnections, which often causes delays due to concentration points between frame relay providers

(vi) Separate power sources for equipment with generator or uninterrupted power supply back-up

(vii) Separate connections to back-up locations

(viii) Regular use of multiple facilities in which traffic is continually split between the connections; and

(ix) Separate suppliers for hardware and software infrastructure needs.

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

– Establish service level agreements that address contingency measures and change management for services provided;

– Ensure that primary and back-up telecommunications paths do not share a single point of failure

– Establish processes to periodically inventory and validate telecommunications circuits and routing paths through comprehensive testing.

(h) **Some vendors offer a drop-ship service as an alternative to occupying the standby site.** That is, in the event of equipment failure, for instance, they will drop off a replacement rather than insist the client occupy the standby site, with all the inconvenience that may involve. But it is essential that a site survey is undertaken to ensure they can be parked on the required site. Most commercial standby sites offering IT and work area recovery facilities do not guarantee a service: the contract merely provides access to the equipment. Although most reputable vendors will negotiate a Service Level Agreement that specifies the quality of the service, it is rarely offered.

It is important to ensure that a bank's service will not suffer from unacceptable downtime or response. The vendor may have skilled staff available – but this is rarely guaranteed and they come at a cost. In terms of cost, there may be additional fees to pay for testing, on invocation of a disaster, and for occupation in a disaster. The vendor charging structure also needs to be carefully considered.

(i) **Outsourcing Risks:** In theory a commercial hot or warm standby site is available 24 / 365. It has staff skilled in assisting recovery. Its equipment is constantly kept up to date, while older equipment remains supported. It is always available for use and offers testing periods once or twice a year. The practice may be different. These days, organizations have a wide range of equipment from different vendors and different models from the same vendor. Not every commercial standby site is able to support the entire range of equipment that a bank may have. Instead, vendors form

alliances with others – but this may mean that a bank's recovery effort is split between more than one standby site. The standby site may not have identical IT equipment: instead of the use of an identical piece of equipment, it will offer a partition on a compatible large computer or server. Operating systems and security packages may not be the same version as the client usually uses. These aspects may cause setbacks when attempting recovery of IT systems and applications – and weak change control at the recovery site could cause a disaster on return to the normal site.

Among the questions banks need to consider are:

- *Is the vendor financially sound?*
- *If the recovery site is occupied when a bank want to invoke the same, where and how the bank does the recovery?*
- *How does the vendor define—disaster– on what conditions the bank can invoke?*
- *How quickly can the bank occupy the recovery site on invocation?*
- *How much will the annual subscription cost?*
- *How much are invocation fees?*
- *How much will it cost to test?*
- *How much testing time is allowed?*
- *Can the vendor personally cover the full range of our equipment and telecommunication needs now?*
- *If not, how will these needs be met?*
- *Does the vendor have standby generators and uninterruptible power supply adequate to maintain the whole installation?*
- *Does the vendor have alternate telecommunication suppliers with separate routing?*
- *Will the vendor keep in step when the bank buys new equipment?*
- *Will the vendor support aging equipment for as long as the bank would need it?*
- *Can a bank's equipment at the vendor site?*
- *Will the vendor drop-ship small equipment at my site to save me having to relocate to the recovery site in the event of hardware failure or loss of a single component?*
- *If so, will they charge extra or is this included in the annual subscription?*
- *Is the location of the standby site safe for staff?*
- *Is the recovery site convenient for public transport?*
- *Does it have rest, shower and catering facilities for staff?*
- *Does it have adequate parking space?*
- *Is the site secure, and will the bank's data remain confidential?*
- *What are the qualifications and skills of the vendor's support staff?*
- *Are they certified as members of the professional bodies like DRII or BCI?*
- *Will the vendor's support staff help the bank recover? If so, how many?*
- *Are there sufficient vendor staff to handle multiple invocations?*

- *Will the vendor's support staff help the bank to test?*
- *Does the recovery site agreement contain a Service Level Agreement specifying availability, reliability and performance?*
- *Does the institution have in place quick and reliable access to expertise for tracking suspicious behavior, monitoring users and performing forensics?*
- *Is there a system of automatic reporting to the authorities concerned – such as the RBI/ IDRBT/ CERT-In and other institutions whenever such events take place?*

Most standby site vendors provide sound service at reasonable cost and are genuinely dedicated to assisting their clients. They have an enviable record of successful recoveries. But, as in any industry, there are a few unscrupulous suppliers. It is the responsibility of the IT manager to ensure effective recovery by those vendors, who apply the highest standards, supporting this by a stringent contract, clearly defining service specifications and technical requirements, and service-level agreements**.**

INDUSTRY-WIDE BCP RECOMMENDATIONS

A holistic BCP would incorporate all dimensions of the banking industry including the financial authorities (Reserve Bank of India), the financial institutions (banks) and the financial market infrastructure. Industry level coordination for contingency planning and management efforts of the individual institutions in the area of operational risk is critical to strengthen the operational resilience of the Indian financial system.

Most important industry-wide recommendations are:

- Establishing an **industry-wide alarm and crisis organisation** (in which the key market participants and the most important providers of infrastructure services are represented. The heads of BCP from the participating institutions can make up the top level of this crisis organisation, with the lower levels forming a network between those responsible for the areas of liquidity, large-value payments, retail payment transactions and IT. Any of the institutions can invoke the alarm organisation by activating the level affected).
- A **website** for industry-wide BCP related information for the benefit of constituents of the industry can be considered.
- **Reviewing** the extent to which the RBI and the Individual banks, can act on behalf of one another in exceptional situations like:

  – Proving funds to other banks customers

  – Waving charges over other banks ATM usage

  – Honoring cheques of other banks

- Intensifying contacts with the telecommunications and IT Infrastructure providers to the Industry
- Examining the extent to which institutions can provide reciprocal support in the event of a crisis
- Banks may consider allowing customers of one bank to use ATM networks of other banks for cash withdrawals with charges being borne by the parent bank.
- Banks may consider waiving off penalties to be levied on delay of in-payments of Treasury deals.
- Banks may consider making a agreement wherein in need of BCP a participatory

Bank will accept request (for a treasury deal / forex transaction/ fixed deposits/ loan) upto a pre-agreed limit on email/ communication basis and accept the required Contract Note/ Promissory Note / Mortgage/ other legal documents at a later stage.

- Based on the above Industry wide recommendations and BCP testing scenarios, the Industry as a whole should look at conducting a BCP drill on a periodic basis to ensure that the BCP plans and measures are updated and effective individually as well as industry wide business continuity. Such initiatives should be taken up by the Industry wide consortium as proposed at the start of this section. For example the testing could include a BCP scenario where a particular city/ processing hub is unavailable for a day. This would involve a calling for a BCP measure by all banks, government organizations, support service providers like Telecom companies, Infrastructure providers, etc.
- The Industry driven alarm and crisis management team as discussed above should ensure that the Industry wide plans are formulated post consultation with all stake holders, these plans are implemented, tested and updated periodically with the changing Industry scenario.
- There are programmes in the US like the Telecommunications Service Priority System (TSPS), Government Emergency Telecommunications service (GETS) and Wireless Priority Service Programme (WPS) for provision of priority telecom availability and recovery services during exigencies for critical infrastructures and institutions. Similarly, Government of India may declare banking sector including financial markets as critical infrastructure and consider instituting such special measures for enabling conduct of critical banking services and market transactions during exigencies.

BCP Considerations for Systematically Important Payment Systems:

- Payment systems are essential for smooth transferring of funds amongst banks and buyers / payers. In times of disaster important payment channels also act as mediums of transmitting shocks across the Industry. These payment systems (also termed as Systematically Important Payment Systems) become critical for industry wide BCP considerations.
- Banks should consider giving special consideration to systemically critical process and systems like clearing, settlement, custody and payment processing (RTGS/ NEFT)
- This may involve identification of the core markets (e.g., money markets, government securities, foreign exchange, commercial paper, equities, and derivatives) and essential functions supporting these markets (e.g., trading, brokering, transaction execution)
- Banks should consider it essential to identify the highest level of operational resilience that will be required to ensure basic functioning i.e. minimum level service of these processes so that BCP is functional for the Industry involving all major financial institutions. *Banks should decide on alternatives, incase a BCP has to be invoked:*

  – Switching over to an alternative payment site

  – Shifting time slots for RTGS and NEFT payments

  – Sending these request to an agreed fall over ‘Service Provider’

  – Having a manual process planned which will take care of critical processing over phone, fax, etc form the alternative site

– Having duplicate hardware ready which can take care of limited requirements

– For all of the above the current systems should have a mechanism in place to facilitate overriding the queue of requests, so as to prioritise processing to those identified as critical/important.

– Banks should consider having BCP requirements of these systems explicitly mentioned in Vendor Contracts, where applicable.

– Banks should consider streamlining its processes to International Standards from ISO, IEC and BSI for strengthening the payment system processes and ensuring a higher level of Business continuity.

– Banks should consider having a multi-skill team from across the Industry trained and ready to take care of these processes with increased focus/concentration. As a BCP measure banks should consider having a dedicated and trained team ready to handle these processes at all times.

The above guidelines for Infrastructure aspects will play a critical role in co-coordinating the effort with help of service providers and industry participants. Hence, as described in above, similar considerations must be given to not just the payment system but:

- Underlying Infrastructure (Telecom and Internet providers and use of dial up when leased line fails)
- Support staff
- Secondary process and alternative service providers

– Banks should also consider having a collateral or security pool arrangement for scenarios of extreme BCP, which can be accepted Industry wide.

– Banks should also consider putting to test the fall over plan for payment systems in the above mentioned Industry wide considerations.

ANNEXURE:

Annexure B: Suggested training needs to management IT infrastructure

KEY RECOMMENDATIONS

1. A bank's Board has ultimately responsibility and oversight over the business continuity planning activity of a bank. The Board approves the Business Continuity policy of the bank.A bank's Senior Management is responsible for overseeing the business continuity planning process which inter-alia includes determining how the institution will manage and control identified risks, prioritising critical business functions, allocating knowledgeable personnel and sufficient financial resources to implement the BCP.
2. A senior official needs to be designated as the Head of BCP activity/function.
3. Since electronic banking has functions which are spread across more than one department, it is necessary that each department understands its role in the plan and the support required to maintain the plan. In case of disaster, each department has to be prepared for the recovery process aimed at protection of the critical functions. To this end, it would be helpful if a set up like the BCP Committee is charged with the

implementation of the BCP in an eventuality and all departments expected to fulfill their respective roles in a co-ordinated manner. Hence, a BCP/Crisis Management Committee consisting of senior officials from various departments like HR, IT, Legal, Business functions, Information Security needs to be instituted

4. There needs to be adequate teams for various aspects of the BCP at Central Office level as well as individual Zonal/Controlling Office and branch level, as required. Among the various teams that can be considered, based on need, include incident response team, emergency action and operations team, team from particular business function, damage Assessment team, IT teams for hardware, software, network support, Supplies team, team for organizing logistics, relocation team, administrative support team, coordination team
5. Banks should consider various BCP methodologies and standards, like BS 25999 as inputs for their BCP framework.
6. BCP should include measures to identify and reduce probability of risk to limit the consequences of damaging incidents and enable the timely resumption of essential operations. BCP should amongst others, consider reputation, operational, financial, regulatory risks.
7. Failure of critical systems, or interruption of vital business processes, could prevent timely recovery of operations. Therefore, banks must fully understand the vulnerabilities associated with interrelationships between various systems, departments, and business processes. These vulnerabilities should be incorporated into the Business Impact Analysis, which analyses the correlation between system components and the services they provide.
8. People aspect should be an integral part of a BCP. Generally, plans are often too focused on the technical issues, therefore, it is suggested that a separate section relating to people should be incorporated, including details on staff welfare, counseling, relocation considerations, etc.
9. *Pandemic planning* needs to be incorporated as part of BCP framework of banks.
10. Banks must regularly test BCP to ensure that they are up to date and effective. Testing of BCP should include all aspects and constituents of the Bank i.e. People, Processes and resources (including Technology).
11. They should involve their Internal Auditors (including IS Auditors) to audit the effectiveness of BCP and its periodic testing as part of their Internal Audit work and their findings/ recommendations in this regard should be incorporated in their report to the Board of Directors and Senior management
12. The institutions should also consider having a BCP drill planned alongwith the critical third parties in order to provide services or support to continue with pre-identified minimal required processes.
13. Banks should periodically move their operations (including people, processes and resources(IT and Non-IT)) to the planned fall-over /DR site in order to test the effectiveness of the BCP and also gauge the recovery time needed to bring operations to normal functioning. Banks should also perform 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.
14. BCP should be maintained by annual reviews and updates to ensure their continued effectiveness
15. Banks should also consider having unplanned BCP drill, wherein only a restricted set of people and certain identified personnel may be aware of the drill and not the floor/business personnel.

16. Detailed requirements relating to procedural, infrastructural and HR related aspects of BCP have been provided so that banks can improve BCP processes helping generate best outcomes.
17. Requirements in respect of various types of testings like table-top, call tree, simulation, component and complete have been indicated.
18. The are many applications and services in banking system that are highly mission 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.
19. The solution architectures of DC and DR are not identical for all the applications and services. Critical applications and services, namely the retail, corporate, trade finance and government business solutions as well as the delivery channels are having the same DR configurations whereas surround or interfacing applications do not have the DR support. Banks will have to conduct periodical review with reference to the above aspect 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.
20. 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 etc.
21. Periodic checks with reference to ensuring data and transaction integrity between DC and DR is mandatory. This could be accomplished by doing the same during lean periods such as the week end or as a part of the EoD / BoD process. .The report on such conformity could be submitted to the in-charge of the BCP/DR of the banks on a regular periodical basis and deviations if any, promptly addressed.
22. Values chosen for the RTO and RPO often mimic the industry practice and are not derived from first principles. Therefore, the DR drills that are conducted periodically have to ensure that the above parameters are strictly complied with. It would be optimal to get the RTO and RPO outlines checked by the IS Audit and further ratified by obtaining customer / user feedback for the first time. Thereafter a random check of these could be done to ensure that these are in tune with the requirements and / or expectation of customer as well as user of the systems
23. DR drills currently conducted periodically come under the category of planned shutdown. Banks have to evolve a suitable methodology to conduct the drills which are closer to the real disaster scenario so that the confidence levels of the technical team taking up this exercise is built to address the requirement in the event of a real disaster.
24. It is to be ensured that the support infrastructure at the DC and DR, namely the electrical systems, air-conditioning environment and other support systems do not have a single point of failure and do have a building management and monitoring system to constantly and continuously monitor the resources. The monitoring of uptime has to be made as per the requirements and agreements with the respective vendors. The same requirements have to be taken care of in case the DC/DR set up is in an outsourced location or a common shared set up as well.
25. Success of a BCP depends on the effective data replication mechanism followed between DC and DR, which is again directly related to the requirements of the banks. The process implemented for the data replication requirement has to conform to this

with no compromise to data and transaction integrity and should ensure seamless resumption of operations to the maximum extent possible. This should be conformed to in the DR simulations and reported accordingly to the Top Management as well.

26. Given the need for drastically minimising the data loss during exigencies and enable quick recovery and continuity of critical business operations, banks may need to consider near site DR architecture. Major banks with significant customer delivery channel usage and significant participation in financial markets/payment and settlement systems may need to consider having a plan of action for creating a near site DR architecture over the medium term (say, within three years).
27. Banks should set in place standardised reporting templates for informing senior management on weaknesses identified through testing or other means, development of action plans, allocation of needed resources, and follow-up reviews to ensure that remedial actions have been effective. Reports should be based on various security metrics typically obtained by systematic and focused log analysis as indicated in information security chapter.
28. A sufficiently large “question bank”, related to security health of the organisation, should be prepared and given to RBI's inspection teams. A random subset of these queries could then be given to the bank's IT or security teams and related personnel, for eliciting answers in quick time.
29. An industry-wide alarm and crisis forum or organisation (in which the key market participants and the most important providers of infrastructure services are represented) may be established. BCP heads from the participating institutions can make up the top-level of this organisation, with the lower levels forming a network between those responsible for the areas of liquidity, large-value payments, retail payment transactions and IT. Any of the institutions can invoke the alarm organisation by activating the level affected. Various recommendations relating to measures banks can consider during exigencies have been provided in the report.
30. A website for industry-wide BCP-related information for the benefit of constituents of the industry can be considered.
31. There are programmes in the US–Telecommunications Service Priority System (TSPS), Government Emergency Telecommunications service (GETS) and Wireless Priority Service Programme (WPS)–for the provision of priority telecom availability and recovery services during exigencies. Similarly, Government of India may declare banking sector, including financial markets, as critical infrastructure and consider instituting such special measures enabling conduct of critical banking services and market transactions during exigencies.