International Journal on Arts, Management and Humanities **1**(1): 73- 80(2012)

ISSN No. (Online): 2319 – 5231

The Implementation of Disaster Management by Indian Banks

Munish Sabharwal & Prof. Anoop Swarup

Shobhit University, Meerut (UP)

ABSTRACT

The main objective of this research paper is to observe whether the selected Indian Banks have any effective Disaster Management System with reference to Disaster Avoidance, Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP) as per RBI guidelines and other international standards. This was pursued by conducting structured interview of branch heads of the selected 16 scheduled banks of Meerut (U.P.). The researcher with the help of a questionnaire inquired from the branch heads of selected banks and compared the responses with the desired state using GAP Analysis Worksheet. The study indicated that the most of the banks selected by the researcher in his research backup its data at a Remote offsite location, have a BCP / DRP Plan available with them on software but they do not apply Disaster Management System as per RBI -"Guidelines on information security, Electronic Banking, Technology risk management and cyber frauds" and other international standards. The study concludes by providing recommendations to the Indian Banks.

KEYWORDS: Disaster Management, Disaster Avoidance, Disaster Recovery Plan (DRP), Business Continuity Plan (BCP), Basel Committee on Banking Supervision (BCBS), Data backup.

INTRODUCTION

Disaster' is defined as a crisis situation causing wide spread damage which far exceeds our ability to recover [1].

The basic types of computing disasters:-

Natural disasters- like earthquakes, floods, hurricanes, etc.

Manmade disasters- like war, bomb blasts, chemical leaks, etc.

Accidents can range from a devastating fire or a plane crashing into data center wiping out a crucial block of data.

The most sinister, and frequently the most catastrophic from of disaster, is deliberate: a disgruntled employee or ex-employee seeking revenge by trashing or stealing key data or introducing a debilitating virus. Also in this category are the possibilities of corporate espionage or damage from hackers. The phases of all disasters be it natural or manmade, are the same.

Disaster management is the discipline of dealing with and avoiding risks. It involves preparing for a disaster before it happens, disaster response (e.g. emergency evacuation, quarantine, mass decontamination, etc.), as well as supporting, and rebuilding society after natural or human-made disasters have occurred.

Disaster Management Act 2005 define disaster management as a continuous and integrated process of planning, organizing, coordinating and implementing measures which are necessary or expedient for (1) prevention of danger or threat of any disaster (2) mitigation or reduction of risk of any disaster or its severity or consequences (3) capacity building (4) preparedness to deal with any disaster (5) prompt response to any threatening disaster situation or disaster (6) assessing severity or magnitude of effects of any disaster (7) evacuation rescue and relief and (8) rehabilitation and reconstruction.

Business Definition for Disaster Management

"…the actions taken by an organization in response to unexpected events that are adversely affecting people or resources and threatening the continued operation of the organization".

Disaster Management for Banks and Financial Institutions: It involves disaster avoidance, disaster recovery and business continuity planning. They are explained by the researcher as below:

Disaster Avoidance: Disaster avoidance is a series of measures designed to prevent, detect, or contain potentially calamitous incidents. It is a component of business continuity planning, which stresses an organization need to have its critical business services available at all times.

Disaster Recovery: Disaster Recovery can be defined as the organization's ability to get back into business quickly after an event that disrupts the flow of information. This is done through a set of pre-planned, coordinated, and totally familiar procedures with an established set of priorities [2, 3].

The disaster recovery is the concept of "failsafe". That is, the bank's ability to survive the disaster it has so valiantly tried to avoid. The disaster recovery plan is extremely necessary to the survival of a bank.

Disaster Recovery Planning (DRP) is a very complex and labor-intensive process; it therefore requires redirection of valuable technical staff and information processing resources as well as appropriate funding. In order to minimize the impact such an undertaking would have on scarce resources, the project for the development and implementation of disaster recovery and business resumption plans should be part of the organization's normal planning activities.

Business Continuity Planning: BCP is the process whereby financial institutions ensure the maintenance or recovery of operations, including services to customers, when confronted with adverse events such as natural disasters, technological failures, human error, or terrorism.

The objectives of a BCP are to minimize financial loss to the institution, continue to serve customers and financial market participants, and mitigate the negative effects disruptions can have on an institution's strategic plans, reputation, operations, liquidity, credit quality, market position, and ability to remain in compliance with applicable laws and regulations. Changing business processes (internally to the institution and externally among interdependent financial services companies) and new threat scenarios require financial institutions to maintain updated and viable BCPB [4].

The difference between Disaster Recovery and Business Continuity: Disaster recovery is the process by which you resume business after a disruptive event. The event often refers to major disruption like a flooded building, Fire, earthquake or the terrorist attacks on the World Trade Center, which disrupt an entire installation or something small, like malfunctioning software caused by a computer virus. Disaster Recovery is REACTIVE; its focus is to pick up the pieces and to restore the organization to business as usual after a risk occurs. The issue of Business Continuity certainly arises when Disaster Recovery is required.

In daily practice Business Continuity often refers to disaster recovery from a business point-of-view, or dealing with simple daily issues like illness or departure of key staffers, supply chain partner problems or other challenges that businesses face from time to time such as a failed disk, failed server or DB, possibly a bad communications line. It is often referred to as the measure of lost time in an application, possibly a mission critical application. It is a plan that will allow the organization to continue generating revenue and providing services – although possibly with lower quality – on a temporary basis until the company has regained its bearings.

Business Continuity is PROACTIVE; its focus is to avoid or mitigate the impact of a risk. Despite these distinctions, the two terms are often married under the acronym BC/DR because of their many common considerations.

REVIEW OF LITERATURE

The World Trade Center attacks on September 11, 2001 brought about never-before-imagined catastrophes which completely changed the perception of BCP preparedness.

Consequently, the Federal Reserve, Securities and Exchange Commission, Office of Comptroller of the Currency and the New York State Banking Department released a white paper in April 2003 which identified three business continuity objectives as having special importance for all financial institutions:

- Rapid recovery and timely resumption of critical operations following a wide-scale disruption

- The ability to recover and continue operations following the loss or inaccessibility of staff in at least one major operating location
- A high level of confidence, through ongoing use or robust testing, that critical internal and external continuity arrangements are effective and compatible.

The Basel Committee on Banking Supervision (BCBS) [2003] released a publication which provided that all banks should have in place *contingency and continuity plans* to ensure that they could continue to operate on an on-going basis and limit losses in the event of a severe business disruption [9].
Jadhav Anil & Rajni Jadhav [2004] in their study suggests that the banks as well as customers have a serious concern about the security of Internet access to client account which is the biggest challenge. Banking through the Internet is increasingly becoming necessary rather than innovative tool and with consumer demand banks have to upgrade and constantly think of new innovative customised packages and services to remain competitive [8].
The Basel II Framework identified and broad types of operational risk events having the potential to result in substantial losses which included continuity risk events such as damage to physical assets, business disruption and system failures, loss on account of external all fraud such as computer hacking, etc.
The Reserve Bank of India (RBI) had recognized the importance of BCP way back in 1998 when it released a guidance note [1998] for management of banks to evaluate the adequacy of controls in relation to risks related to Computer and telecommunication systems including interruption risks. This was followed by the release of a report on "Information Systems Audit Policy" [2004] including "Information Systems Security Guidelines" by the RBI in 2001 which provided indicative standards and procedures for Audit of Information Systems including BCP as a component [11, 13].
The RBI in its Guidance note on "Management of Operational Risk" [2005] has stressed the need to establish a disaster recovery and BCP for technology related risks as a part of ORM framework. The RBI, in its circular on operational risk management and business continuity Planning" [2005], clearly states that the responsibility for effective migrated BCP rests with the Board of Directors and the management and has listed a set of minimum requirements for effective BCM by banks. The circular also required banks to disclose information relating to major failures of critical systems customer segment/services impacted due to failures and steps taken to avoid such failures in future. The RBI, in its guidelines on "Outsourcing of Financial Services by Banks" in 2005, has mandated banks to ensure that the service provider has a BCP and the same is regularly and maintained [4, 7, 10, 12].
V. Radha [2008] in her study discussed about the technology based opportunities that the thieves take advantage of and how to limit the frauds by building the future technology accordingly [14].

METHODOLOGY

The research work was conducted with the objective to observe whether the selected Indian Banks have any effective Disaster Management System with reference to Disaster Avoidance, Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP) as per RBI guidelines and other international standards.
The research work was conducted to prove the assumption that the Indian Banks do not apply Disaster Management System as per RBI guidelines and other international standards.

Scope of Research: Since all banks follow the norms of the RBI and the computerization by banks is done as per the recommendations of committees formed by the Central Bank from time to time, therefore their policy for implementation of the computerization in branches of a particular bank are same anywhere. Therefore, the area of research chosen by the researcher is Meerut city, as it is a well developed city having branches of most of the banks.

Population: The researcher has focused his research only on the scheduled banks. The scheduled banks are SBI & its six Associates, 19 PSU's, OTHER PUBLIC SECTOR BANK- IDBI Bank Limited, 14 OLD PRIVATE SECTOR BANKS, 7 NEW PRIVATE SECTOR BANKS, 36 FOREIGN BANKS, Regional Rural Banks (Total 82 Banks are their but in UP only 7 are present and in Meerut only 1 with only one branch). There are 53 Urban Cooperative Banks, 31 State Cooperative Banks, 371 District Central Cooperative Banks and 93413 Primary Agricultural Societies in India.
Sample Design: Since the population size is very big it was not feasible to study the entire population, so the researcher decided to go for a sample survey. In order to get a holistic representation, the researcher has used

stratified sampling and scheduled banks categorized by RBI have been divided into groups referred to as strata on the basis of the Total Turnover of the banks.

Sample Size: The total number of banks selected by the researcher is 16 (Sample size- 16). The list of selected banks is as shown in table.

List of Banks selected as sample			
S. No.	**Bank**	**S. No.**	**Bank**
1	SBI- State Bank Of India	9	South Indian Bank
2	PNB- Punjab National Bank	10	Nainital Bank
3	CBI-Central Bank of Indian	11	ICICI Bank
4	Syndicate Bank	12	HDFC Bank
5	Andhra Bank	13	Axis Bank
6	Punjab & Sind Bank	14	Yes Bank
7	Bank	15	Sarva UP Gramin Bank
8	Federal Bank	16	Zila Sahkari Bank, Meerut

Research Design

Data Collection: Since all the information could not be obtained from secondary sources therefore for the collection of firsthand information for primary data, the researcher prepared a questionnaire containing various questions regarding the computerization in banking.

The branch for a bank is selected by the researcher taking into consideration the size and business of the branch, which ensures that the branch will be fully computer equipped as per bank norms. The list of selected branches in Meerut of selected 16 scheduled banks.

Then the researcher conducted well scheduled interviews and the respondents are asked to complete the questionnaire by verbally responding to questions in the presence of the researcher, through a face-to face structured interview.

The Researcher also noted on-the-spot observations by visiting the branches of the banks and using their various products and services like ATM's, Tele-Banking, SMS Banking, Net Banking, Mobile Applications, POS Terminals, Credit and Debit cards of various banks.

Ana

lytical Tool: The mainly quantitative data produced by this questionnaire was analyzed through GAP analysis. Gap analysis is a tool that helps organizations compares actual state with potential state. At its core are two questions: "Where are we?" and "Where do we want to be?".

Gap analysis compares the Current State of banks (as per the collected data) with the Desired State of the banks (considering the various Guidelines, Rules and Regulations of RBI, the international Guidelines as well as Data from international organizations like World Bank etc.) and it is presented with the help of GAP Analysis Worksheets etc.

ANALYSIS & FINDINGS

1. **In Q.No.1 the researcher inquired about whether the Bank backup its data at a Remote offsite location and compared the responses with the desired state:**

GAP ANALYSIS WORKSHEET 1.0			
CURRENT STATE		**DESIRED STATE**	**GAP**
Name of the Bank	**Does the Bank (Branch) backup its data at a Remote offsite location**		
SBI	**Yes**	**As per Reserve Bank of India Department of Banking Supervision, Central Office, Mumbai - "Guidelines**	**Nil**
PNB	**Yes**		
CENTRAL BANK	**Yes**		
SYNDICATE BANK	**Yes**		

ANDHRA BANK	**Yes**	**on information security, Electronic Banking, Technology risk management and cyber frauds" - All Banks must backup their data at a Remote offsite location**	
P & S BANK	**No (Only for CBS Branches)**		
IDBI BANK	**Yes**		
FEDERAL BANK	**Yes**		
SOUTH INDIAN BANK	**Yes**		
NAINITAL BANK	**Yes**		
ICICI BANK	**Yes**		
HDFC BANK	**Yes**		
AXIS BANK	**Yes**		
YES BANK	**Yes**		
SARVA UP GRAMIN BANK	**Yes**		
ZILA SAHKARI BANK	**No**		**When the bank starts computerization then it must implement remote data backup facility.**

All the banks selected by the researcher in his research excluding Zila Sahkari Bank backup its data at a Remote offsite location as is visible from GAP analysis worksheet 1.0 and Punjab & Sind Bank only takes backup of data at remote location for CBS Branches only.

2. In Q.No.2 the researcher inquired about whether the Bank has any Disaster Avoidance Plans for its branches and compared the responses with the desired state:

GAP ANALYSIS WORKSHEET 2.0			
CURRENT STATE		**DESIRED STATE**	**GAP**
NAME OF THE BANK	**Does the Bank's (Branch) have any Disaster Avoidance Plan?**		
SBI	**Yes**	**As per Reserve Bank of India Department of Banking Supervision, Central Office, Mumbai - "Guidelines on information security, Electronic Banking, Technology risk management and cyber frauds", the banks must have a preventive programme to reduce the likelihood that a bank's operations will be significantly affected by a pandemic event.**	**Nil**
PNB	**No**		**Disaster Avoidance Plan as a Preventive measure is required**
CENTRAL BANK	**Yes**		**Nil**
SYNDICATE BANK	**Yes**		
ANDHRA BANK	**Yes**		
P & S BANK	**No**		**Disaster Avoidance Plan as a Preventive measure is required**
IDBI BANK	**No**		
FEDERAL BANK	**Yes**		**Nil**
SOUTH INDIAN BANK	**Yes**		
NAINITAL BANK	**No**		**Disaster Avoidance Plan as a Preventive measure is required**
ICICI BANK	**Yes**		**Nil**

HDFC BANK	**Yes**		
AXIS BANK	**Yes**		
YES BANK	**Yes**		
SARVA UP GRAMIN BANK	**Yes**		
ZILA SAHKARI BANK	**No**		**Disaster Avoidance Plan as a Preventive measure is required**

The data of GAP analysis worksheet 2.0 suggests that SBI, CBI, Andhra Bank, ICICI Bank HDFC Bank, South Indian Bank have Disaster Avoidance Plans but PNB, Syndicate Bank, Axis Bank, Punjab & Sind Bank and Zila Sahkari Bank does not have any Disaster Avoidance Plans.

3. In Q.No.3 the researcher inquired about whether the Bank has any Disaster Recovery Plan (DRP) or Business Continuity Plan (BCP) and compared the responses with the desired state:

GAP ANALYSIS WORKSHEET 3.0			
CURRENT STATE		**DESIRED STATE**	**GAP**
NAME OF THE BANK	**Bank (Branch) has any Disaster Recovery Plan (DRP) or Business Continuity Plan (BCP)**		
SBI	**Yes**	**All the banks as per Reserve Bank of India Department of Banking Supervision, Central Office, Mumbai - "Guidelines on information security, Electronic Banking, Technology risk management and cyber frauds" must have a Disaster Recovery Plan (DRP) or Business Continuity Plan (BCP)**	**All the banks do have a Disaster Recovery Plan (DRP) or Business Continuity Plan (BCP) documented on software but as observed by the researcher in several branches, during situations when there is loss of connectivity, then the BCP is not used in branches as the Managers & employees feel that if they make the payment or authenticate the transaction, which is not valid or the customer plays fowl due to CBS facility, then they may be held responsible.**
PNB	**Yes**		
CENTRAL BANK	**Yes**		
SYNDICATE BANK	**Yes**		
ANDHRA BANK	**Yes**		
P & S BANK	**Yes (Only for CBS Branches)**		
IDBI BANK	**Yes**		
FEDERAL BANK	**Yes**		
SOUTH INDIAN BANK	**Yes**		
NAINITAL BANK	**Yes**		
ICICI BANK	**Yes**		
ingHDFC BANK	**Yes**		
AXIS BANK	**Yes**		
YES BANK	**Yes**		
SARVA UP GRAMIN BANK	**Yes**		
ZILA SAHKARI BANK	**No**		**Business Continuity Plan (BCP) must be put in place**

The data of GAP analysis worksheet 3.0 suggests that all the banks selected by the researcher in his research excluding Zila Sahkari have Bank Disaster Recovery Plan (DRP) or Business Continuity Plan (BCP), which is available on their information System.

4. In Q.No.4 the researcher inquired whether the Bank setup any Disaster avoidance, Disaster recovery committees at branch level and compared the responses with the desired state:

GAP ANALYSIS WORKSHEET 4.0			
CURRENT STATE		**DESIRED STATE**	**GAP**
NAME OF THE BANK	**Bank (Branch) Setup any Disaster Avoidance, Disaster Recovery committees at branch level**		
SBI	**No**	**As per Reserve Bank of India Department of Banking Supervision, Central Office, Mumbai - "Guidelines on information security, Electronic Banking, Technology risk management and cyber frauds", the banks must have a preventive programme to reduce the likelihood that a bank's operations will be significantly affected by a pandemic event, for which the banks needs to setup Disaster Avoidance, Disaster Recovery committees at branch level**	**None of the banks setup any Disaster avoidance, Disaster recovery committees at branch level.**
PNB	**No**		
CENTRAL BANK	**No**		
SYNDICATE BANK	**No**		
ANDHRA BANK	**No**		
P & S BANK	**No**		
IDBI BANK	**No**		
FEDERAL BANK	**No**		
SOUTH INDIAN BANK	**No**		
NAINITAL BANK	**No**		
ICICI BANK	**No**		
HDFC BANK	**No**		
AXIS BANK	**No**		
YES BANK	**No**		
SARVA UP GRAMIN BANK	**No**		
ZILA SAHKARI BANK	**No**		

The data of GAP analysis worksheet 4.0 clearly suggests that all of the banks selected by the researcher in his research do not setup any committees for Disaster avoidance and Disaster Recovery at their branches.

Hypothesis Testing: The analysis as described in GAP analysis worksheet 1.0 to GAP analysis worksheet 4.0 proves that almost all the Indian Banks backup their data at a remote offsite location and almost all the Indian banks have a BCP / DRP Plan available with them on software but do not apply Disaster Management System as per RBI -"Guidelines on information security, Electronic Banking, Technology risk management and cyber frauds" and other international standards. This proves that the Hypothesis : "The Indian Banks do not apply Disaster Management System as per RBI guidelines and other international standards" assumed by the researcher, is TRUE.

CONCLUSIONS & IMPLICATIONS

❖ All the banks selected by the researcher in his research excluding Zila Sahkari Bank backup its data at a Remote offsite location and Punjab & Sind Bank only takes backup of data at remote location for CBS Branches only.

◆ All the Indian banks have a BCP / DRP Plan available with them on software but they do not apply Disaster Management System as per RBI -"Guidelines on information security, Electronic Banking, Technology risk management and cyber frauds" and other international standards.

◆ SBI, CBI, Andhra Bank, ICICI Bank HDFC Bank, South Indian Bank has Disaster Avoidance Plans but PNB, Syndicate Bank, Axis Bank, Punjab & Sind Bank and Zila Sahkari Bank do not have any Disaster Avoidance Plans.

◆ All the banks selected by the researcher in his research excluding Zila Sahkari have Bank Disaster Recovery Plan (DRP) or Business Continuity Plan (BCP), which is available on their information System.

◆ All of the banks selected by the researcher in his research do not setup any committees for Disaster Avoidance and Disaster Recovery at their branches.

Implications:

❖ Banks should have Disaster Avoidance Plans which must be reviewed quarterly.

❖ All of the banks must compulsorily setup committees for Disaster Avoidance and Disaster Recovery at their branches.

❖ RBI must make provision & technological adjustments to encourage bank employees to use BCP as and when required.

REFERENCES

1. Disaster Management", accessed on Dec 2011, <http://www.cyen.org/innovaeditor/assets/Disaster_Management_Notes_and_Questions.pdf>
2. Beth Verity, "Guide to Network Cabling Fundamentals", Canada: Cengage Learning, (2003) pp-269
3. "Disaster Recovery", accessed on Dec 2011, <http://www.netsmithusa.com/pdf/netsmithusa_wp_dr.pdf>
4. "Business Continuity Planning", accessed on Dec 2011, http://www.bankinfosecurity.com/ten-steps-to-effective-business-continuity-plan-a-186/p-2
5. "Difference Between Disaster recovery and Business Continuity", accessed on Dec 2011 <http://oracle.ittoolbox.com/documents/disaster-recovery-plan-vs-a-business-continuity-plan-16494>
6. Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System (April 7, 2003).
7. Basel Committee Publication No. 96: Sound Practices for the Management and Supervision of Operational Risk (February 2003).
8. Jadhav A.S., Mrs. R.A. Jadhav, "Status of e-banking in India", National annual convention of CSI (2004).
9. Basel Committee on Banking Supervision – International Convergence of Capital Measurement and Capital Standards: A Revised Framework (June 2004).
10. RBI circular Ref. DBS.CO.ITC.BC. 10/31.09.001/ 97-98 on "Risks and Control in Computer and Telecommunication Systems" (February 4, 1998).
11. RBI Information Systems Audit Policy for the banking and financial sector (October, 2001).
12. RBI Guidance Note on Management of Operational Risk (October 2005).
13. RBI circular Ref. RBI/2004-05/420 DBS.CO.IS Audit.No. 19/31.02.03/2004-05 on 'Operational Risk Management; Business Continuity Planning (2004).
14. V. Radha, "Preventing Technology Based Bank Frauds", "*The Journal of Internet Banking and Commerce*", Vol. **13**, No. 3. (Dec. 2008) pp.22-29.