2. RESEARCH METHODOLOGY

2.1 The problem

The Financial Reforms that were initiated in India in the early 90s and the globalization and liberalization measures brought in a completely new operating environment to the Banks. Banking sector reforms have been based on five fundamentals:

- Strengthening of prudential norms and market discipline.
- Appropriate adoption of International benchmarks.
- Management of organizational change and consolidation.
- Technological upgradation.
- Human resource development.

The arrival of foreign Banks and Financial Institutions, the setting up of a number of private banks and the measures of de-regulation that encouraged competition has led to a situation where the survival of those who do not join the race will become difficult. Unless the state-of-the-art IT was introduced as early as possible, winning new business and even holding on to the old one will become increasingly difficult.

Simultaneously, the importance of effective MIS for control of operations and of maintaining customer and business/industry data bases for strategic planning has also surfaced; while Banks are looking at Data warehousing, Data mining, Business Restructuring etc. as most essential things to have as early as possible, they are taking urgent steps to computerize the operations in their administrative and controlling offices (viz. head/zonal/regional offices) as well as the data collection machinery, so as to evolve an effective MIS. In this phase, the new communication revolution sweeping the nation and the world has come in extremely handy, as the communication infrastructure has improved significantly and the Internet
technologies are available to network branches at a relatively low and affordable cost with a high degree of reliability.

Reserve Bank of India constituted a committee under the chairmanship of Dr. C. Rangarajan. For the purpose of computerization, the committee selected the various important areas relating to customer service, internal-decision-making process, productivity and profitability.

Services and products like "Anywhere Banking" "Tele-Banking" "Internet banking" "Web Banking" "e-banking", “e-commerce”, “e-business” etc. have become the buzzwords of the day and the Banks are trying to cope with the competition by offering innovative and attractively packaged technology-based services to their customers.

Banks today need to leverage modern technologies such as internet, mobile, smart cards, biometric authentication in their efforts to provide banking and financial services to the rural populace, and thereby create hitherto unprecedented economic opportunities.

The uninterrupted banking service is the most important. These services are now fully based on technology, but technology itself can’t ensure the effectiveness of the services. The management of technology and its disasters is another key point on which adequate attention must be given.

Data integrity and protection is a daunting task these days for businesses in the banking sector. Not only has the amount of data created every day exploded, but there are also compliance requirements under various regulations.

Banks were among the earliest adopters of information technology in the business world. They embraced the benefits of computers almost from the birth of the high-tech industry.
Disasters are sudden, calamitous events that bring great damage, loss or destruction, whether through natural or technological causes. Typically, they cause loss of life and property and social and economic disruption.

Technological disasters are usually associated with man-made infrastructure, and are typically accidental, though the rise in global terrorism has awakened populations to the risk of purposeful calamities, whether nuclear, biological, radiological or chemical. Examples of technological disasters include chemical or nuclear plant explosions, mining accidents, and major train derailments involving hazardous materials.

The disaster can take place in the following manner:

- Hardware failure
- Software failure
- Network failure
- Electricity failure
- Human Factors
- Natural Factors
- Riots
- Terrorism

There are certain types of risks associated with the above mentioned disasters:

- Transaction/Operational Risk
- Technology Risk
- Credit Risk
- Liquidity Risk
- Strategic Risk
- Reputation Risk
A proactive approach is critical to banks and financial institutions. Planning is vital to disaster recovery because the primary objective is to avoid problems before they occur.

Disaster recovery is of particular importance for the banks in a locality hit by crisis - more so than other businesses - because their services are in great demand during times of community disaster. The average bank is multi-plat formed, with multiple locations and varied operations and computer applications.

Business recovery has moved beyond recovering computer systems to restoring and recreating business processes. The outage of whole departments needs to be considered, and how work and information will flow from one place to another or from department to department should be studied.

While some businesses could afford a 24 to 48 hour computer shutdown, that length of recovery window is horrific for a bank and a worst-case scenario. If a bank loses its funds transfer function for a day or two, it could be very damaging to business. Banks tend to run many critical applications simultaneously, so recapturing data lost at the point of failure as quickly as possible is crucial.

Disaster recovery will continue to evolve with the banking industry. As banks and financial institutions become more sophisticated technology users, disaster recovery solutions will follow. But banks and financial institutions must plan for disaster recovery every step of the way.

The key to successful disaster recovery is what happens long before a disaster strikes. With a realistic recovery plan, properly tested and committed to by senior management, banks can effectively maintain operations while providing for the safety of people and assets.
2.2 Research Methodology

In this study efforts have been made to study the present policies of Technological Disaster Management of selected public sector banks and their branches. I have collected information regarding technological status of few well known banks in India i.e. State Bank of India (SBI), Punjab National Bank (PNB), Bank of Baroda (BOB) and United Commercial Bank (UCO). Information about the actual incidents of disasters in these banks have also been collected.

There are various documents circulated in banks regarding disaster management. The system and procedure to face such situation is also set. Internal audit also check the documents relating to disaster preparedness in branches.

The firm belief of the researcher that all the circulars and documents regarding management of disasters actually do not pertain to disasters. In fact the definition of disaster and its interpretation in banking has been taken very lightly. If there is any break in connectivity from central data server, it is treated as disaster.

If there is any problem in normal functioning of ATM machine, it is also treated as disaster. The role of branch staff and services available at that time is the major contribution in disaster management guidelines in bank.

If we think about the disasters seriously, it will require more concentration on all aspects of disaster. There is a need to understand the situation of disaster in banks to that appropriate arrangement can be made to meet the challenges of such worst situations.

Therefore, it was basic requirement of my research which inspired me to know the actual position of disaster management in banks.
The researcher few experienced officials of the several bank to know the actual position of disaster management in their bank.

Every officer narrated that to face disasters various instructions have been issued by their bank to the branches to face the situation of disasters and these were common in all banks. When question was raised about the disaster and their intensity, they simply replied that the disasters are those, which have been described by the bank in its circulars.

Questions were as follows:

- Suppose data centre of your bank is destroyed, then how the data will be recovered?
- The reply was: we have disaster recovery site at another place.
- Researcher again asked: suppose the disaster recovery site is also destroyed?
- The answer was: this is a silly question, how can it be? This is not possible.

The researcher interview with some bank officers was started with curiosity, but ended with incomplete reply as they could not accept the situation of total destructions of their primary data centre primary as well as at alternate disaster recovery centre.

The researcher was surprised to know that there is no arrangement to face the situation for complete loss of data.

The attack of 9/11 at WTC brought many new dimensions of disaster. The preplanned strategy of facing such situation is not sufficient because the impact of every disaster does not reflect as it was expected.
During the interview with the bank officials the researcher was told about the actual incidents in their branches. To the researcher opinion these incidents will depict the actual disaster management in some banks.

A big branch of a big bank was working in branch computerization module. The data relating to this branch was not centralized at bank level. It was branch level computerization. The backups were being taken as per instructions of the bank and system & procedures were also followed. Backup DATs were being kept in other branch as per disaster recovery manual.

One day, the server could not be started. There was an error while booting hard disk. The branch manager then called the AMC vendor to solve the problem. The AMC vendor visited branch and found that hard disk was crashed and it was to be replaced with new one. The branch manager was relaxed because the backup of data was available in day wise backup DATs. After installing the new hard disk and operating system, the AMC vendor asked to provide backup DAT of previous day. The DAT was restored and that took more than 1 hour to restore the data. But when the application software was invoked, there was no data found in the server.

The AMC vendor was surprised to note that the process of restorations was completed and it was apparently successful. Then the restore log file was checked. It was found that there was message for every restored file that the restoration was unsuccessful and data could not be read from DAT.

The branch staff was relaxed and customers were told to wait for few hours. But the situation arose after restoration of DAT, made everybody impatient. The backup DAT of previous days were checked but no data could be restored. The matter was then referred to their IT department. After the detailed enquiry, it was revealed that no data backup was successful for entire last one year. The backup DAT were kept day wise, month wise and year wise
which were overwritten by the time and every DAT was found as bearing as NULL data.

In another incident, backup of data for the last one year could not be restored completely. Only general ledger balances of all accounts could be found in backup media. The transaction history of last two months could not be restored. The customers were asked to wait till the transactions in their account is rebuild from the reports available in other locations.

These two incidents are sufficient to prove the zero level of bank’s data if the backup is not restored completely.

The branch computerization has been migrated to Core Banking Solution where the data is located centrally. Backup of data is also taken centrally. The alternate site of live data is also maintained to face the disasters.

But the possibilities of loss of entire data cannot be ruled out. Therefore, the researcher decided to study the various components and impacts of all type of disasters by dividing these into sub categories as interruption, breakage in services, crisis and two class of disaster so that each situation of disaster can be evaluated and banks can take appropriate steps to face such kind of worst situation with possibilities of zero data and growing or retrieving all required data from various sources so that normalcy is restored in minimum time with least cost and efforts.

The study of actual technological disaster incidents in banks provided the researcher with the actual picture of management in banks and effects of such disasters on the public and customer services. Information relating to various disasters and reasons thereof was also collected and analyzed in such
a way so that relevant conclusions can be drawn for effectiveness of recovering from such disasters.

This study also required personal interviews of bank officers and their experience with such disasters. Questionnaires for customers and employees of the banks were also prepared to study the common aspects of such disasters.

Information was also collected of selected banks to observe their disaster management policy and actual recovery period so that a practical approach to the concept could be suggested.

2.3 Objectives of Research

Banks are serving a wide range of their customers like individuals, business firms, Corporations and Government and other institutions in many ways. There is a need to ensure smooth functioning of the bank and their branches in case of major disasters which unexpected and unwarranted, to maintain the faith of the public in reliable banking.

The researcher observed many incidents when ATM of a bank is not working. Sometimes shutter of such ATM is closed and people can’t do anything, but they blamed the modern technology and carelessness of the bank.

There have been many occasions when branches of a bank can’t work for the whole day, even more than a day due to failure of their computer system or connectivity.

The disaster management in banks is very important for the continuity of their business and smooth functioning of the economy. If any bank fails to provide immediate relief to its customer in case of disaster, it loses the confidence and trust of the public.
It is assumed that every bank is fully aware of the importance of technological disaster management. This study will prove to be helpful to assess the present level of disaster management and effectiveness of these measures.

Disaster Management is completely a matter of concern of individual banks. Every bank has its own Technology Department and experts. Despite all efforts, incidents of technological disasters are increasing considerably. This research work will certainly find out the true picture of Technological Disaster Management in Banks.

The difference between interruptions and disasters can better explain the intensity of effects of such incidents. The objectives of this study are to find out the actual status of preparedness against the known and unknown disasters so that appropriate steps can be taken to improve the quality of management regarding fighting against disasters.

2.4 Review of Literature

There are a few books and articles including RBI directives in this regard. There are few books on disaster management. The main source of information of disasters and their management is circulars issued by the respective banks. Some banks have published their disaster management strategies on their web site also and in their annual reports. There are also some articles on technological disasters in banks. The brief description of such books & articles is given here.

R K Uppal : 2006

*Indian Banking Industry and Information Technology*

This book examines the impact of IT on the growth and performance of a cross section of it on the growth and performance and growing competition among the banks is forcing the nationalized banks to provide
prompt and reliable customer service and offer a variety of Hi tech banking product/services.

*R K Uppal & Rimpi Jatana* : 2007

**E banking in India Challenges and Opportunities**

This book contains 12 articles by scholars specializing in the area of banking. It will be useful in this research to understand recent technological development in Indian banking.

*R.P. Nainta* : 2005

**Banking System Frauds and Legal Control**

This book highlights evolution of the banking system, Reserve Bank of India, nature of crime in the banks, legal provisions and the methods of safety and security measures, etc.

*Prof. D Suryachandra Rao* : 2008

**Banking Reforms in India An evaluative study of the performance of commercial banks**

The book provides a comprehensive review of banking reforms and shifts that have taken place in the perceptions, policies of commercial banks. The main theme of the book is to present a systematic analysis of the impact of Banking Sector Reforms in the areas of efficiency and profitability of commercial banks.

*Benson Kunj Kunju* : 2008

**Commercial banks in India Growth, Challenges and Strategies**

The book describes the remarkable changes since the nationalization of 14 major commercial banks in 1969 banking sector in India & about the transformation itself into a vibrant financial service sector with many innovative and technology driven at their end.
In additions of the above, there are some articles which have also been published. A brief review of such articles is given here under:

- Vepa Kamesan (2004) Former Deputy Governor RBI studied the benefits of knowledge in banking and considered that any new technology enabled process can act as a differentiator or a competitive edge for some level of time. He also pointed out major issues related to customers.

- Nitin Khanapukar (2008) in his article has pointed out that Banks need an efficient Business Continuity Plan (BCP). Government across the world has recognized the critical need for banks to keep operating even in the face of disasters.

- Website www.bankofbaroda.com highlights the IT-Infrastructure & IT-Enabled Services at bank of Baroda.
  - Banks IT-enabled Business Transformation Programme
  - Bank’s State – of the – Art Data Centre.
  - Wide Area Network(WAN)
  - Branch Computerization
  - ATM Network
  - ATM-cum-Debit cards
  - Tele Banking, PC Banking, Any Branch banking
  - Mobile Banking
  - RBI’s National Electronic Funds Transfer (NEFT)

- Financial Sector Technology vision “Document of Department of Information Technology”. It discusses the major landmarks regarding task of promoting automation & banking sector to improve customer service, Bookkeeping, MIS, productivity. Besides this, steps have been initiated for providing a platform for transmission of electronic messages using common standards facilitating “Straight through Processing” (STP) in the form of structured.
Financial Messaging System (SFMS) the vision document discuss focus areas like

- IT and IDRBT(Institute for development & research in Banking Technology)
- IT for Financial Sector
- IT for government related functions
- Risk Management of E- Banking Activities(E-Banking booklet) discuss about various types of risks involved in online banking like operational risk, credit risk, technological risk etc. It also gives the information security control measures and administrative control measures and administrative control measures to prevent technological disasters like Dual Controls, Error Checks etc…

➢ **Vadlamani Ravi** in his article highlights the *use of advanced statistics and Computer Science* to measure, mitigate and manage various risks associated with banks. It talks about various statistical and Computer Science algorithms for quantifying the risk whose information can then be used by the management team in hedging the risk through various countermeasures as applicable.

➢ **Rangarajan Committee Report (1998)** talks about *Applications of Information Technology in Banks in India*. It has opened flood gates for global economic activity. Dr. C. Rangarajan (Former governor of RBI) drew the plan for computerization & mechanism in Banking Industry for 1985-1989.

➢ According to Munish Sabharwal and Prof. Anoop Awarup, Disaster Recovery (DR) and Business Continuity Planning (BCP) are two different concepts.
DR is a reactive process by which we resume a disruptive event like flooded building, Fire, earthquake or the terrorist attacks on the World Trade center.

BCP is proactive plan which allows the organization to continue generating revenue and provide service.

The Basel Committee on Banking Supervision [2003] released a publication which forced the banks to have contingency and continuity plans to ensure that they could operate on ongoing basis and limit loss in the event of a server business disruption.

Jahav Anil & Rajni Jadhav [2004] in their study suggests the banks as well as customers have a serious concern about the security of internet access to client account which is the biggest challenge. RBI realized the importance of BCP in 1998 where it released a guidance note for management of banks to evaluate the adequacy of controls in relation to risk related to Computer and Telecommunication systems including interruption risks. This was followed by the release of a report on “Information System 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.

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.

Questionnaire was prepared and analyzed through GAP analysis. GAP analysis is a tool that helps organizations compares actual state with potential state. At its core there are two questions: “Where are we?” and “Where do we want to be?” GAP analysis compares the current State of banks with desired
state of banks (considering various Guidelines, Rules, 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 Worksheet etc.

<table>
<thead>
<tr>
<th>Question/Bank</th>
<th>SBI</th>
<th>PNB</th>
<th>BOB</th>
<th>UCO</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>2</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>4</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Q.1 Does the Bank (Branch) backup its data at a Remote offsite location?
Q.2 Does the Bank’s (Branch) have any Disaster Avoidance/Prevention Plan?
Q.3 Bank (Branch) has any Disaster Recovery Plan (DRP) or Business Continuity Plan (BCP)?
Q.4 Bank (Branch) Setup any Disaster Avoidance, Disaster Recovery committees at branch level?

There are also some overseas firms which provide disaster management services to the banks. These firms have described various stages of disasters and their management strategy and also providing services for effective disaster management.

2.5 Research Gap

There is hardly any research in technological disasters in banks. It has been assumed that the technology itself is not responsible for the disasters, but people who take care of such technology are responsible for the disasters. There are some books which describe the technological aspects in banks. Some articles also narrate the various aspect of technology in the banks. Each and every Bank has its own written documents for the disaster recovery.
It was observed that the actual study regarding technology and disasters in banks had not been done so far. The disaster takes place when there are no alternatives of the technology. This study will work out the role of technology in banks and their alternatives and will help Indian PSBs to form an efficient data recovery plan.

2.6   Hypotheses

**Main-Hypothesis:** of this research study is that the effective policy of Management of Technological Disasters is being followed by the banks and their branches to provide prompt and uninterrupted customer services to the customers.

**Sub-Hypothesis:** is that either the policies relating to technological disasters are not being framed by the Banks or the policies/measures are not effectively being managed by them.

2.7   Source of Data

**Primary Data:**
- Separate questionnaire is prepared and was distributed to bankers, employees and customers of banks. There response is served as primary data for this research.

**Secondary Data:**
- Head Offices of Various Public Sector Banks
- Bank Journals
- Books
- News Papers and Magazines
- Internet.
2.8 Tools of Research

- Study of Incidents of some disasters in banks
- Personal interviews & their common results
- Assessment of effectiveness of various techniques

2.9 Scope of The Study

There are so many types of disaster. Some of these are men made and some are natural. The technological disasters refer to only those, which relates to modern technology. This study has taken care of all such technological disasters in banks which have been occurred or could be occurred. The technical aspects of various apparatus which are being used by the banks have been assessed.

The role of hardware as well as software has been assessed in this research. The human behavior, which affects all the activities of banking business and technology was also studied and analyzed.

2.10 Rationale of The Study

The rationale of the research is to assess whether the present policies and management of technological disasters are sufficient or not, to assess the requirement of new techniques or policies? Whether the reasons behind the disasters are poor policies or their improper implementation? These rationales have been proved as the basis of my study, research and outcomes.

2.11 Contribution to The Discipline

This study will be helpful to the banking industry for their better management. As the banks are known as the flag holder of modern technology, the development of the technology depends upon the better utilization and effectiveness of such technology. So, the researcher think that her research work will contribute to the betterment to the banking industry as
well as to the technology which is being used by the banks or to be used by the banks in future.

2.12 Contribution to The Society

Banks are dealing in finance, but these are economical & social institutions too. The uninterrupted services rendered by the banks present well equipped and well technological advanced institutions of the society. Every section of society needs banking facilities. If banks can serve them in disasters also, the society can be relaxed and affirm their belief on the modern technology and its development. If banks can serve the society more affectively, the contribution to the society will be assessed automatically.

2.13 Contribution to The Nation

Banks are the strongest institutions for the growth of the economy of the nation. If banks are technologically strong, they can serve the nation in better way and the faith of other countries in Indian financial institution will be grow. Thus this study will contribute the technical soundness of the nation.

2.14 Limitation of The Study

There are 26 public sector banks in which 19 are nationalized bank. State Bank of India and its 6 subsidiary banks have autonomous status. When we talk about public sector banks, we have to look into all the 26 banks. The study about all the 26 banks was time taking. Therefore, the data of selected public sector bank have been collected and analyzed on the basis of study of these selected public sector banks.

The study was kept limited to the context of Indian Banking industry because the actual incidents of some disaster could be studied. However, some incidents of the other banks which have published in news papers etc. have also been studied to present a comprehensive picture of the technological disasters.