8: SUMMARY, CONCLUSION & SUGGESTIONS

8.1 Summary

In a Bank hundreds of activities take place daily and these include thousands of transactions. Transactions can be relate to Check, Payment, Deposit, Transfer In, Transfer Out, Credit Card (Pay Bills), Investment, Loan, Saving account, Current account etc. There are also various functions in banks like providing customer service at premises and providing services on alternative channels. To manage these transactions banks require applications to satisfy their customers fully. And these applications run on some technologies.

Technology is a branch of knowledge that deals with the creation and use of technical means and their interrelation with life, society and environment. The power of technology is used for material gains. It is used in mobiles, computers, TV, microwaves, at home for fast results. It is also used in banks in computers, servers, web sites to deal with day to day banking transactions. Technology means, the way of performing activities with more efficiency in lesser time with improved skills. It may be a machine, it may be a process.

Technologies (struts, SAP, mainframes etc… are based on computer languages like java, .net, Cobol etc… These languages have set commands which are given to computer to function in a specific manner. Collection of commands is called a program and collection of programs with interface, input and output is called an application. These applications are used to minimize the time and effort of bankers and customers with lesser chances of error.
• Funds transfer (within and outside the bank)
• Interbank Mobile Payment Services (IMPS)
• Enquiry services (Balance enquiry/ Mini statement)
• Cheque book request
• Demat Enquiry Service
• Bill Payment (Utility bills, credit cards, Insurance premium), Donations, Subscriptions
• Mobile Top up
• M Commerce (Top up of Tatasky, BigTV, SunDirect, DishTV, DigitalTV and Videocon d2h connections, SBI life insurance premium)
• All Current/ Savings Bank Account holders in “P” segment are eligible.
• Transaction limit per customer per day is Rs.50, 000/- with a calendar month limit of Rs.2,50,000/-
• All customers can avail the Service irrespective of their telecom service provider.
• The Service is free of charge. SMS/GPRS cost will be borne by the customer.

Mobile Banking Service over SMS: is available on all phones (java/non java) with/without GPRS connection. No need to download the application. Ordinary SMS charges are applicable. The following functionalities are available:
• Enquiry Services (Balance Enquiry/Mini Statement)
• Mobile Top up
• DTH Top up/ recharge
• IMPS- Mobile to Mobile Transfer
• Change MPIN
• All Current/ Savings Bank Account holders in “P” segment are eligible."
8.1.1 Manual Banking to Computerized Banking

The first bank of world was setup in 1397 and the first bank of India in 1786, but the oldest bank which is now working in India, was setup in 1806. Thus, the story of manual banking in India is older than 206 years. The manual banking was migrated on branch computerization banking during the period 1995 to 2000 and from branch computerization to CBS banking from 2001 to 2005. Therefore, it took more than 200 years to migrate on technology from manual banking. The components of technology in Banking are as under:

- Dependency of Technology
- Power
- Hardware
- Software
- Data
- Connectivity

The intensity of each component can be assessed in the light of its substitute or alternative which are available or can be adopted if primary or original source is not available or fails.

Power

The most important component of technology is power. The primary source of power is power generating units either in govt. sector or in private sector. Power generated by the source is available at prescribed rates.

There can be situation when power from original or primary source is not available temporarily. If power from primary source is not available temporarily, it can be obtained from UPS. UPS is temporary source of power supply if it has backup for required period or hours. Such backup can be available in UPS if required number and capacity of batteries are installed in UPS. The other source of power supply is Generator. Generator can be used...
for temporary power supply. The generator can work on fuel or gas. If fuel or
gas is not available, the generator cannot work and power supply cannot be
restored for other components of technology.

Therefore, power is dependent on producer, batteries, fuel. Hence,
power alone cannot be considered the main component of technology. The
sub components are also required to ensure the interrupted power supply.

**Hardware**

The second important component of technology is hardware. Hardware
includes CPU and storage device. If speed of CPU is not compatible to the
operating system or application software, the hardware cannot work
efficiently. Another important part of hardware is hard disk. Hard Disk stores
the data for processing and future use. The storage can be done on external
device. Thus, hardware is dependent on CPU and storage device.

**Software**

Software is also known as important or essential component of
technology. Hardware cannot work without software. Hardware is only a
machine and it can work only after it speaks in its language i.e. machine
language. Software can be two types i.e. operating system and application.
Operating system enables the hardware in working condition along with all its
attached devices. Application or program is another type of software. Every
type of processing is done by application software which has been designed
and developed for specific purpose. The flow and logics of application
software decides the outcomes of the application. Therefore, software is also
an important part of technology which depends on operating system.

**Data**

The information stored in computers and retrieved when required is an
essential part of technology. If there is no use of data, the importance of
technology is zero. The processing and findings of current information does not require any disaster management. The application software is only an important part of technology. But, in this, study data is considered as an important part of banking. Therefore, in this case, technology is dependent on data. Another part of data is its backup. If backup of data is not taken, the retrieval is not possible in case of need. Therefore, data is dependent on backup i.e. application software and storage media.

**Connectivity**

The primary source of external connectivity is INSAT. The owner of connectivity is BSNL. If there is any problem in INSAT or BSNL, the connectivity get effected. BSNL provides connectivity through leased line and ISDN line. If there is any problem in these lines, then connectivity gets affected. The reasons for problem can be natural disaster or technological disaster at their end. Sometimes, cabling of BSNL is cut due to various reasons. Therefore, primary connectivity depends upon various factors.

Secondary source of connectivity is VSAT, LAN, WAN. This type of connectivity can be said as relayed connectivity. VSAT receives the signals from INSAT. If VSAT is not working nor have some technical problem, then the connectivity gets affected. In the same way, if LAN is not working properly, the internal connectivity is not restored.

Internal connectivity also depends upon the devices like Switch, Hub, modem, Cable, ports, connectors etc.

This means that connectivity is not absolutely independent. It depends upon some other facts as mentioned above.
Therefore, the various components of technology are dependent on other factors or devices. If these factors or devices are not working efficiently, the role of technology is also become poor.

Now, question arises, if there is any break in technology at any level, can bank provide customer service as usual?

As discussed above, the every part or component of technology is not independent absolutely. However, the replacement available at that time can be used in most of cases which is available in plenty in the market.

Power can be procured from different sources because which are available in the market.

Hardware can be replaced with new one or with other better configurations because these are available in the market.

Software can also be arranged from the developers or can be developed as new or fresh software for required applications.

Connectivity can also be made available internally. This can be done through cables. If data are made available in branch server, the services can be provided for branch customers.

But, whenever the role of data is to be assessed, the replacement of data is not available in the market. Therefore, the data is not dependent on any other component. It cannot be brought from other sources.

This independency can make data as a master technological essential among all the other components.
The disaster recovery or management plan can provide adequate guidance for procurement of other components of technology. But the data can be only original of backed up data. Backup of data means data safety, security and retrieving when required.

If there is zero availability of original as well as backup data, then customer service cannot be provided with the help of borrowed data or rental data.

The word disaster means some mishap or damage occurring suddenly, causing loss to humans, buildings, organizations etc. data, connectivity, information & machines.

Technological Disaster means interruption in normal working of machines or technology. The example of technological disasters as under:

- Hard disk crash resulting in loss of critical data.
- System resource failure e.g., connectivity failure etc., resulting in the unavailability of resources for computing.
- Virus attacks resulting in loss of critical data/stoppage of critical applications.
- Hacking of core banking application resulting in misuse of important data.
- Network attacks resulting in unauthorized access to confidential data.
- Hardware theft resulting in monetary loss.
- Fire resulting in loss of software, data, and hardware.
- Electricity failure because of natural calamities, like storms, heavy rains, grid problem at service provider side, hard disk failure, data corruption, application instability.
- Human error such as an administrator accidentally erasing data or crashing a network.
When disasters take place, technologies are first to be affected. On the contrary disasters can be controlled by the technology itself. Disasters can be natural and human. Natural disasters like flood, earth quake, cyclones, volcano, drought etc. and Human disaster like Banking Frauds, Terrorism, Hardware Failure, Software Failure, Network Failure, Electricity Failure.

Suppose there is flood in the city and because of that there is no electricity. No electricity means no computer and no computer means no application. The customer who has urgent work in bank has to wait for hours till electricity comes or some alternative arrangements are made available to complete their banking transactions in a smooth way. Thus Natural disasters can cause Technological disasters.

Due to Terrorism the World Trade Centre attacks Sep11 2001 more than 50 domestic and international organizations got effected. These organizations include brokerage house, a bong house, international or domestic commercial banks. They were physically collapsed completely but because of contingency planning they could be placed into operation immediately upon the destruction. Thus it can be conclude that terrorism also causes technological disasters. Banking frauds like cyber crimes, forced thefts etc are also increasing these days causing harm to ATMs, banks, and society. Managing the after effects of these disasters as fast as possible should be our effort.

Management means handling something in a systematic and efficient way with the full control over activities in a right direction & restoration of normal situation in minimum time with minimum loss to the users. If one technology fails, rest can work independently or without any break. If electricity fails, UPS can work smoothly If UPS fails, Generator can work. It means there are alternatives of electricity supply.
Management of technological disasters means restoration of normal working either by providing alternate methods or by adoption of alternative technology or by manual or providing parallel services through other centers. We can also call them Management of Technology in such a way so that these can be operationlize in disasters too.

8.2 Conclusions

A DR solution that is typically deployed between a primary production site and a DR site goes through various states of usage. The disaster recovery can be undertaken by Disaster Recovery Managers (DRM). DRM goes through a discovery phase where all the subsystems of a DR solution, their relationship, and the dependency between the primary and DR systems are mapped. The DR process execution logic uses this information to sequence steps and synchronize execution of the logic.

DRM is the only DR-focused solution that integrates with primary and DR components, maps their relationship and co-relates events, automates the DR process, and also monitors DR health, all of which needs knowledge of primary and DR systems. Traditional enterprise management solutions are used to keep the production systems up and efficient. This includes monitoring, performance, and routine operations on production servers and applications.

As part of solution deployment, DRM discovers the primary and DR infrastructure, including platforms, applications, and replication technologies. DRM compares discovered subsystems and their relationships against known and best-practices DR solutions, such as Oracle protection using EMC SRDF, IBM DB2 using HADR, or SAP using MaxDB. DRM offers several pre-packaged DR solution signatures that enable easy and quick deployment and DR process automation that is tested and ready to use.
Financial institutions are dependent on IT applications for running their daily operations. With disaster recovery assuming critical significance in the business world today,

The type of DR solution can be driven by the outcome of the business impact analysis (BIA). A BIA enumerates the risks that a business could possibly face and their likely impact on the business.

A three-site DR solution addresses the considerations. A zero RPO requirement requires data to be replicated synchronously. Synchronous replication requires that when data from the server is written to storage, a copy to the local storage and a copy to the remote storage be saved on the storage before the application is able to continue.

The network delay incurred in writing a copy to the remote storage limits the distance that synchronous replication can be used for. Typically, the distance that synchronous replication can be deployed is between 60 and 100 kms. Hence, to meet the zero data loss requirement, the bank chose to have a near site. To cover the scenario in which a regional event could impact the primary site and the near site, a DR site was chosen to be in a different region of the country.

DR process for this three-site solution. Monitoring also provided real-time reports on application level RPO.

DRM recognizes the various phases of the DR life cycle that includes data replication during normal times and the automation required to failover in times of primary outages and for conducting DR drills to test the recovery readiness of the solution. Recovery Automation Library provides readymade templates that make implementation of automation of failover and the DR drill for all the applications easy and time-bound. To redirect the transactions
of business users to the DR site in case of an outage at the primary site, the bank uses the network NATing technology. Software interfaced with Cisco routers to automate the process of changing the *NAT tables* so that user access to the application is redirected to the DR site transparently.

There are many tools in the market to monitor and manage a production environment and interfaces with systems across two or more sites to give DR monitoring and management capabilities in a single dashboard.

Every supported DR solution signature in the product ships with failover workflow for application recovery and switchover and switchback workflows for DR drills. Using these workflows ensures that the solutions deployed followed industry best practices and that recovery automation met software quality control metrics.

DR drills are the best way to exercise a recovery plan. The big challenge in doing drills is the time and resources required to prepare for it. “Extensive co-ordination is required among the different teams to ensure that configurations are correct.

Unpleasant surprises during DR drill can be bad news. DRM Drill Manager conducts pre-flight checks to ensure that parameters such as access, permissions, and environment are correct. If they are not correct, the user is alerted, thus enabling them to fix the gaps before the commencement of the drill. This dramatically improves the success rate of the drills.

The DRM Drill Manager enables the automation of IT workflow. It *integrates* tightly with *heterogeneous technologies* and enables automated execution of the steps required to test various technologies.
Summary, Conclusion & Suggestions

Automation is easy

It can be started with built in switchover and switch back workflow or build your own using the Recovery Automation Library (RAL), a repository of recovery steps for various technologies that can be very easily put together as a workflow. Automated workflow dramatically reduces the need for experts, reduces the time required to execute the drills, and eliminates operator errors.

The life cycle approach to disaster recovery that DRM solution takes addresses the DR challenges that banks face, thereby increasing IT availability. DRM solution automates application recovery and helps banks reduce IT downtime by recovering application within set SLAs. It addresses issues in the banking industry where the run book may be out-of-date and the steps don’t match the configuration.

It also provides the bank with critical data on recovery timeframes, measured against the RTO, and the amount of data loss, measured against the RPO. More importantly, it enables banks completely automate their DR drill process, thereby saving time and resources.

Requirement of DR Drills

Drive DR operational efficiency, lower the cost of DR operations, and enable agile IT organization.

Reduce IT down time due to outages by reducing recovery times.
• Meet regulatory requirements of conducting regular drills, as automation enables faster and parallel execution of the DR drill process.
• Save time and resources required to collate data for DR reports by providing ready-made reports.
• Deploy best-practices DR solutions in the shortest time possible through packaged DR templates.

Banking is considered to be the second largest segment for using IT, next to manufacturing. More and more banks are embracing this growing trend of outsourcing to stave off competition. Indian companies need to capitalize on the size of their economy and growth potential, besides leveraging their strong IT infrastructure and cheap labor. The government has to speed up its infrastructure development efforts to maintain the momentum of growth in the outsourcing industry.

Besides, the industry and regulators the government should draft proper data privacy and security norms. The industry needs to move up the value chain, and infrastructure bottlenecks and data security issues must be resolved. All these measures will help the banking industry to unleash its full potential for outsourcing.

**Disaster Recovery Plan**

As bank operations become decentralized, regional operations centers and satellite offices face greater exposure. Bank work groups such as customer service employees serving clients by telephone from remote locations must be part of the overall disaster recovery plan.

The staples of virtually every work group environment - office space, personal computers, telephones, automatic call distribution systems, and other critical office equipment - including those in remote locations - need to be accounted for in the recovery plan.

*Disaster Recovery Planning aims at minimizing loss potentials through the development of capabilities and procedures in the wake of non-speculative interruptions of critical business functions.*
The first objective of DRP is to respond to a disaster potential before it becomes a disaster.

The second objective is to minimize the cost associated with disaster potentials that cannot be eliminated.

Many disasters do not emanate from a single debacle but develop over a period.

Considering the growth in business and dependence on Technology it is necessary that all business units (branches) of Bank must have a DRP. Development of DRP is a structured approach that calls for the following steps:

1. Prepare a comprehensive list of all assets at the branches. The final list should contain all the assets at the branch including software licenses.
2. List out all the threats like Power failure, Fire, Software problems, Hardware failure, and Dial-up connection on network PC etc.

The DRP itself is likely to contain considerable details of corporate operations, systems and procedures. It should cover all foreseen eventualities and must be dynamic, in so far as it must constantly reflect where the organization/branch/data centre is now, not where it was two years or even six months ago. Keeping the plan updated is, therefore, likely to be a continuous monitoring job of a group of persons.

A formal disaster recovery planning exercise needs to be framed and renewed quarterly between each of the CBS branches and their respective controllers. A mid-year review of the branch activities associated with the DRP needs to be conducted by the Controllers. What would be a mistake is to ignore the potential for catastrophic events within the increasingly technological environment in which today's business operates.
Each DRP should become a part of branch document, and a reference be made in the Branch Manager's Monthly Certificate in regard to the compliance of associated activities including testing of the recovery plan procedures. In any case a DRP for the branch should be more exact and holistic, with emphasis on quick recovery following a disaster. The plan should also specify the testing program at quarterly intervals with the involvement of the branch personnel. Copies of the document to be circulated among the DR team members on a ‘need to know’ basis. A Distribution Register to be maintained, listing the identity of the individuals to whom the DRP is distributed. The control numbers and the location of each copy the DRP are also recorded in the Register.

Staff members should be encouraged to suggest improvements to enhance the effectiveness and increase the efficiency of DR operations. Incentive schemes may be introduced to encourage high levels of participation.

### 8.3 Business Continuity Plan (BCP)

*A BCP is a plan that defines the activities to be performed that will ensure continued business operations during any interruption that can affect normal business operations.* It includes events like absence of personnel, power failure, system unavailability and also disastrous event.

Failure of business continuity can be broadly classified into three categories:

- Temporary failure - lasting a few minutes.
- Medium failure - lasting a few hours.
- Long Term failure - lasting more than 24 hours.

This broadly covers the following aspects:

- LAN and WAN connectivity issues.
- Server and Client issues.
Business Operations including Offline Functioning.
- General guidelines on Maintenance.

8.4 Results of Hypothesis Testing

**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 public.

The hypothesis is not approved as the actual disaster is not being faced by the banks. The interruption is being taken as disasters and customers are advised to come later on. The offline functionalities are also not being used. Customers have to wait till the normal situation is restored.

**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 managed by them.

Sub hypothesis is approved. There is well defined, well framed disaster policies on the record and properly documented which available at bank’s web site. Disaster Recovery Plan (DRP) and BCP are being effectively managed by the banks as this is being checked by internal auditors.

8.5 Suggestions

There is need to identify the areas likely to invite a disaster such:

- Environment - Cleanness
- Hardware – Physical & logical Security
- Data-Security & Backup
The environment can be divided in the following sections:

**Temperature**

Temperature should be between 18 to 20 degree to avoid server crash and it should be controlled by installing Air Conditioners. It is preferable to install Split AC instead of Window AC because the compressor and other main components of AC are kept outside the building away from Server room. This will avoid possibility of disaster on account of electrical short circuit.

**Dust**

Server room should be kept free from dust, unused superfluous material. Line printer should be kept at a separate compartment attached to the server room to avoid paper dust coming out of the printer. Vacuum cleaner should be used for dust cleaning.

**Insects**

Anti-pesticide and anti insecticide treatment should be carried out periodically in the server room and eatables or liquids should not be allowed inside the server room.

**Fire**

Fire Detection device must be installed in the building. Ensure strict compliance of No Smoking policy inside the branch premises. Remove combustibles from the proximity of potential ignites. Replace certain types of synthetic carpets, upholsteries, plastics etc with less hazardous equivalents. Arrange for inspection of all electrical devices, extension cords etc., at periodic intervals by expert electricians. Arrange for inspection by the local fire protection officials. Ensure setting up of fireproof partitions of system room. Obtain annual certificate for fire ratings from the appropriate local authority or bank’s engineer regarding the equipment room walls, ceilings and floors. Ensure fire exits are unobstructed and clearly marked. Identify fire
and smoke detectors and ensure that these are working properly. Conduct regular fire evacuation drills to initiate a disaster prevention awareness program within branch staff and customers. Locate fire suppression capabilities such as standpipe/hose assemblies, sprinkler systems and wall-mounted extinguishers. Check for, current inspection and test labels. Arrange for fire insurance policies to be updated with appropriate noting in the branch document.

**Power supply**

The power supply to the building, the location of the power distribution box shall be made known to staff at the branch as also the alternative method of power supply that exists in the event of interruption. Recommendations of electrical experts should be obtained for lightning protection and the capacity of arresters to be located at the point of service entry, for dissipating lightning energy before it causes harm to the power devices. Regular inspection of the equipments needs to be arranged. UPS is one of the components of power support system. It is sized and selected at all branches to support a load required by the hardware, lighting and other equipments. The UPS room should be away from the system room so that any short circuit shall not affect the system room. The branch has to ensure constant monitoring of the function of the UPS, as sudden failure of UPS may create disasters for the branch. The related areas of monitoring are as follows:

A small overhead passage may be created between the system room and UPS chamber to allow free flow of cool air from the air conditioner unit of the system room to UPS to provide optimum operating temperature.

The frequency converter, a component of UPS needs to be inspected periodically to ensure proper operation.
UPS batteries need to be checked/tested periodically to ensure that power reserves will be available. Wherever required, the UPS vendor may be asked to install Simple Network Management Protocol (SNMP) in consultation with the concerned hardware vendor. This checks the battery storage level and notifies users accordingly.

Power distribution panels for the system room used for delivery of conditioned power from the UPS bus to various load devices need to be checked periodically. A diagram of electrical cabling detailing various circuits and respective miniature circuit breakers (MCBs) is displayed inside the UPS room. Instructions regarding switching on and off of the UPS should be prominently displayed inside the UPS room.

Generators of adequate capacity are installed at the branch to cope with prolonged interruption in the power supply.

**Local Area Network**

LAN cabling network is kept separated from the electric cables. The floor of the system room is insulated with non-static material like polyvinyl.

**Water**

Flooding is one of the vital sources for possible disaster at branches. This may result from natural disaster, structural faults within the branch premises, plumbing leakage, and leakage from air conditioners. The branch has to ensure regular check up of the existing facilities to exclude possibility of major disasters. The system room is to be away from the toilet blocks.

**Moisture**

Regular cleaning of the system room and hardware components at the branch with dry cloth would help in keeping off the moisture particularly during monsoon season. The system room may be provided with a
hygrometer to make a note of humidity level and keep it at the stipulated level. Packets of silica gel may also be kept inside the system room, cabinets where DATs (Digital Audio Tape)/floppies are stored.

Physical Access

Branch should assess the existing level of physical security in respect of hardware equipment placed at the system room/branch and plug in the loop holes if any, in order to prevent damage to existing hardware, prevent theft of hardware items and to prevent unauthorized disclosure of information and or data from the system.

Personnel authorized to enter the system room, in branches where the system room is provided, are allowed after making due noting in the System Room Access Register with time, date and purpose of entry.

Virtual Access

This should be ensured by way of password authentication. All the authorized users should be set up in the system and allotted passwords to access the system. Any unauthorized user attempting access to the system will be alerted and the branch should observe such alerts as a hedge against possible intrusion to the system.

Software

It may be ensured that other software like screen savers, free software or unauthorized software are not installed in the server or at the workstations in the branch. It may be ensured that any standalone system with Internet connectivity at the branch is not connected to the CBS network.

Hardware

Operational failure of hardware equipment is one of the common causes of disaster. Server is the most sensitive equipment whose failure may
lead to a complete halt in the system functioning at branches. The branches should ensure that the hardware vendor/AMC vendor carries out periodical Preventive Maintenance job for all the hardware equipments/peripherals.

It is mandatory to have the Anti Virus software installed on the file server as also on the workstations. No workstations should have floppy drive/CD ROM drive.

**Monitoring system resources**

Identified Official should monitor the system resources e.g., free space available in the hard disk.

**Annual Maintenance Contract**

After initiating control measures for accessing to hardware, similar control mechanism needs to be invoked to restrict access to the software for various kinds of users. Meticulous observation of User Rights control measures will help in the safety and security of the entire system.

**DATA**

Data on the Server consists of various items like operating system and Database and application software etc., these should be backed up on to DAT (Digital Audio Tape) everyday as per laid down instructions. This should be ensured by way of keeping separate tapes for all the days. In addition to Tape backups, a CD backup should also be taken every day on re-write CDs. The tapes/floppies can be kept in a Fire Proof Cabinet kept outside and far away from the system room.

**Backup**

The next course of action would be to identify a strategy for safe storage of backed up data. Obviously, the On Site storage strategy is a
preferred one due to easy access to back up data. But this is fraught with risk of timely retrieval of data at the time of disaster.

While identifying the Offsite storage centre, two aspects have to be considered viz., the proximity of the storage centre to the concerned branch and authorization of personnel of the branch for having access to the backup data on tapes/floppies.

The laid down instructions implies that the tape backup and other backups / floppies should be kept at the same branch overnight before it is deposited to the offsite place next morning. In the absence of any of branches in the vicinity of the data backing up branch, a branch of any other commercial bank or financial institution may be designated as storage centre after ensuring safe storage arrangements thereat.

The branch should maintain proper record (Storage Media Record Register) for safe deposit and withdrawal of backup tapes/floppies by authorized personnel. The branch head should peruse this register at periodical intervals. The Controllers, on their visit to the branches, should ensure that the systems and procedure as laid down are being followed in this regard.

The offsite storage centre should be advised to keep proper record for safe deposit and delivery of backup tapes/floppies to authorized personnel only and on must be tested periodically.

The branch users to be advised to post the transactions into the system under ‘Off-line Functionality’ and upload the data as soon as the connectivity is restored, strictly in the manner detailed in CBS guidelines, under confirmation to the Controller.
The branch users to be advised to accept cash deposits from the customers and to maintain records of all such deposits manually in the prescribed manner lay down by the Bank. With regard to withdrawals, the users to print the Deposit and Loan Balance Files of previous day from the Branch or from any of the nearest branch/office and handle withdrawals depending upon merit of each case and basing on the Deposit / Loan Balance File on maintaining records of all such transactions manually, as per the existing instructions of the Bank. Transfer vouchers to be accepted by the branch users and records thereof to be maintained manually, as per the prescribed norms. All such postings are to be made into the system as soon as the connectivity is restored at the branch, under confirmation to the Controller.

The branch users to be advised to perform banking activities from another specified branch, which has been approved by the Controller. Cash transactions, if made at the specified branch, to be handled in the prescribed manner. Charges should be waived for non home transactions relating to this branch.

The names and addresses of the key personnel, vendors, service providers, support officials and also the names and addresses of all the staff of the branch are to be circulated.

**LAN and WAN connectivity issues**

Very often branches experience that they are unable to connect to the data centre system or that certain clients are not functioning. More often than not, the problems are transient in nature and get resolved in the normal course. However, it would be useful for the branch if they could identify the problems and take appropriate action. Branches are advised to study the document carefully and plan their responses to such situations in a systematic and organized manner.
Preliminary analysis to be done by the branch staff before escalating the matter, include:

- Verifying all cable connections is proper and there are no loose connections or connectors or I/O points.
- Verifying power connections and availability to the Router, Switch.
- Verifying whether the network card is functioning.
- Looking for any error messages about cable or network card failure from the system.
- Performing the LAN and WAN connectivity tests.
- Recording error messages in a register for accurate reporting of errors and to maintain records of connectivity failures, with date and time indicated.
- Recording the speed of response in milliseconds as indicated from the output of the ‘ping’ command.

**Server and Client Issue**

This can happen at the branch due to server crash or its non-availability for any other reason. In such instance, branch should contact the vendor immediately and advise IT Department.

These problems can arise due to several causes like component failure, virus attacks, system load, power fluctuations, system software files being corrupted or damaged etc. In all such cases the branch should first contact the vendor or the service provider handling the AMC.

These problems may affect either the server or the clients or both. Some of the possible solutions that can be explored in this event are replacement of server with a standby server if available at short notice.
Local IT department should ensure availability of one or more servers at key points such as Regional Offices, large branches and other remote centers. Existing Bankmaster (P-IV) servers can be configured for this purpose with all required software including Oracle and B@ncs Link and antivirus loaded.

Wherever feasible the vendor may also be requested to provide a standby system of required configuration until the main system becomes available. The services of the vendor should invariably be used for such restoration of server.

Replacement of components (hard disk, memory cards, power supply unit, network cards etc.) should be done by the vendor immediately. Branch should discuss with the vendor the nature of problem and obtain information on expected time of replacement of components.

In case of network cards, however, the vendor may be advised to configure the additional card usually available in the system and restore the original configuration once the new card becomes available. Most of the other components can usually be replaced within a few days. It must therefore be realized that server failure would usually imply delays in restoration ranging from a few hours to several days. Hence an alternate server being made operational immediately or within a short time is the best option.

Reinstallation of operating system and all related system software followed by installation of the application and all associated components can be done at the branch as copies of the Operating Software and all other component software are available at the branch. In many cases it will be necessary to restore certain files only that may have got corrupted. In case of difficulty in this regard, assistance of specialist officials or ITS DEPT officials may be sought.
Virus attack requires updated antivirus software and clean up of the system, before use. The latest virus definitions must be downloaded or obtained from the nearest branch, ITS DEPT or other sources and system updated. Please ensure that only authorized Edition is loaded and updated. The current status of antivirus can be determined by verifying the virus definition date. This can be seen by double clicking on the antivirus icon on the desktop taskbar (far right bottom portion). If the date is not recent (less than a week), it needs to be updated immediately and a scan run to see if any virus has already attacked the system. Any virus found must be deleted or at least quarantined.

**UPS and related issues**

Problems arising from power fluctuations, non-availability of clean power to server and nodes from UPS etc. will require long term solutions. Branches should arrange for a study of the UPS requirements and associated local raw power supply problems and refer to their Controller for appropriate action. In the event of a UPS failure, branch should contact the UPS vendor or AMC holder immediately.

It may become necessary to isolate the server and one or more key client systems from the rest of the systems and arrange to provide power at least to these critical systems. It is advisable to see that separate electrical wiring is done for the sensitive equipment and systems (router, server and key nodes and printers), so that the entire load is distributed appropriately. Branches are cautioned against directly connecting systems and other sensitive equipment to raw power. All power supply to these systems must only be through UPS.

**8.6 Business Operations & Offline Functioning**

The following options are available for continuing operations when the Core Banking systems become unavailable for any reason:
Manual Operations

Using Offline Functionality

Operating through the nearest Core Branch

- It should be the endeavor of the Branch to provide a reasonable level of satisfactory services even in time of disaster. Only proper planning and advance preparation for dealing with such situations can help the branch in rendering continued customer service.

- The disaster recovery plan should contain the situations where next step is not possible. Then, alternate of best solution should be suggested.

- In emergency, data can be available on Internet with ids and password. Every bank is now having its own website for public. There should be a link for disaster arrangements where customer can check their balances. ID and password can be generated at the time of opening of account for view right to all accounts holder.

- The primary data availability is bank’s site or disaster recovery site. Every bank has now provided two sites for their data. The original data is stored at main server on real time basis. The backup is also taken with little delay but every transaction is being recorded at log files and backup process takes care of these log files. Therefore, the original data and backup data is almost the same. If there is disaster at original data site, the backup data can be used as original data after verification from log file.

As per the guidelines of RBI, every bank has to test their disaster site once in a month/half year or yearly to ensure the reliability of backup process.

Another data relating to alternate delivery channels e.g. ATM, Internet banking and mobile banking transactions is also updated on real time basis in all cases except few as there is some ongoing process for updating of such data.
Summary, Conclusion & Suggestions

Total loss of data at primary site as well at backup site

There is a little possibility of deviation in original data due to time lag in alternate delivery data. Now, suppose the original data of the bank is gets destroyed or cannot be retrieved at any cost. At the same time, the backup data is also not available or destroyed. Then what will happen? The answer of this question can be given by the Disaster Recovery Manager intelligently as “the possibility of data lost at original site as well as at backup or disaster site, will be zero.” I have discussed matter with the few bank officials to know the actual position of their banks in case non availability of data. It was told by them that there is “Offline” functionality in bank. Offline functionalities are available in every bank but it is not used. The list of balances of customer accounts is available in report format. If computer savvy staff is asked to deal the customer manually on the basis of this report, they will never ready because it is very hard to turn manual work from smooth computer based transactions. What remedies are available if original as well as backup data is lost and not available at any cost? The disaster recovery planner should take it seriously.

There can be few solution of this problem too.

In case of major disaster, data pertaining to sufferer bank can be merged with other bank and this bank can provide customer service for sufferer bank also.

Data can be uploaded at internet site of sufferer bank or IBA, RBI or IDBRT site so that customer can make enquiry of their account balances to ensure the reliability of the data.

User id and password can be customized with account number and mobile number combination. This facility will be for balance enquiry, therefore, misuse of id and password will not be possible.
As per discussions held with bank officials, it is revealed that every branch in CBS is getting reports of each and every customer account regularly on daily basis. In some bank these reports are received at local server at interval of two hours in one bank. These reports include all static as well as dynamic details of each customer and each account. These reports can be used to create database in case of major disaster and no original data is restored and customer service can be provided, if software can upload this data at local computers to provide information to their customers instantly.

Therefore, the reports now can be treated as the secondary source of data. Thus, the chain of components of technology is complete in all respect.

**Suggested Work Flow in case of Major Disaster**

Disasters are although well defined but can occur in any shape at any time. A suitable work can be suggested keeping in view the available present alternatives. I have kept in my mind that if sufferer bank cannot provide customer services due to major disaster, the other competent bank make be asked by the central bank or Govt. to provide customer services. This will help to strengthen the faith of public in banking system. All these can be done as mentioned in following diagrams.
Figure 8.1 Suggested Component & Work Flow of Banking Transactions

<table>
<thead>
<tr>
<th>Customer</th>
<th>Branch/mode</th>
<th>Facility</th>
<th>Type of Transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer</td>
<td>Own Branch</td>
<td>Every type of Transaction without any Charges</td>
<td>Transaction &amp; Enquiry</td>
</tr>
<tr>
<td></td>
<td>Other Branch</td>
<td>Every type of Transaction with some charges</td>
<td>Transactions &amp; Enquiry</td>
</tr>
<tr>
<td></td>
<td>Other Bank Branch</td>
<td>Every type of Transaction with some charges</td>
<td>Transactions &amp; Enquiry</td>
</tr>
<tr>
<td></td>
<td>Own ATM</td>
<td>Specified Transaction without charges</td>
<td>Transactions &amp; Enquiry</td>
</tr>
<tr>
<td></td>
<td>Any ATM</td>
<td>Specified Transaction with charges</td>
<td>Transactions &amp; Enquiry</td>
</tr>
<tr>
<td></td>
<td>Bank’s Internet</td>
<td>Specified Transaction with or without charges</td>
<td>Transactions &amp; Enquiry</td>
</tr>
<tr>
<td></td>
<td>Bank’s Web site</td>
<td>Only Enquiry</td>
<td>Mobile SMS</td>
</tr>
<tr>
<td></td>
<td>Mobile Van</td>
<td>Specified Transaction with or without charges</td>
<td>Transactions &amp; Enquiry</td>
</tr>
</tbody>
</table>
Figure 8.2 Suggested alternatives in case failure of equipments

<table>
<thead>
<tr>
<th>Equipment</th>
<th>Failure part</th>
<th>Failure type</th>
<th>Alternative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Supply</td>
<td>Electricity Department Supply</td>
<td>Depends on Time</td>
<td>UPS Backup</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Own Transformer</td>
<td>Power Cut</td>
<td>Generator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Voltage</td>
<td></td>
</tr>
<tr>
<td>Outer Connectivit</td>
<td>INSAT/VSAT</td>
<td>Disasters</td>
<td>No remedy but wait</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cable cut</td>
<td>Alternative backup line</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Power Failure</td>
<td>Alternative backup line</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Inefficient Staff</td>
<td>Alternative backup line</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Strike etc.</td>
<td>Alternative backup line</td>
</tr>
<tr>
<td>Internal Connectivity</td>
<td>Router</td>
<td>Not working</td>
<td>Replacement</td>
</tr>
<tr>
<td></td>
<td>Switch</td>
<td>Not working</td>
<td>Replacement</td>
</tr>
<tr>
<td></td>
<td>LAN Cable</td>
<td>Not working</td>
<td>Replacement</td>
</tr>
<tr>
<td></td>
<td>I/ O Box</td>
<td>Not working</td>
<td>Replacement</td>
</tr>
</tbody>
</table>
Figure 8.3 Type of disasters

Hardware
- Main Server → Crash
- Branch Server → Crash
- Clients or Computers → LAN Cards

Software
- Operating system → Disasters
- Application Software → Hard Disk
- Computer Virus → LAN Cards

Natural Disasters
- Earthquake
- Heavy rain or Flood
- Hurricane
- Tsunami

Manmade Disasters
- Fire
- Riot
- Mishandling of Hardware
- Malfunction of Software
Figure 8.4 Suggested alternatives in case of data loss

1. Data lost
2. Backup
3. Reports
   - Creation of Data
   - Merger of data with another Bank
     - RBI
     - IDBRT
     - UID
     - NFS