Unit – 4
Core Banking Solution

CHAPTER 1

CBS BASICS AND ITS WORKING METHODOLOGY

LEARNING OBJECTIVES

- What is Core Banking Solution
- Technology behind CBS
- Comparison of TBA (Total Branch Automation) with CBS
- Data Centre and Network Connectivity
- Functions of IT Department under CBS environment
- Modules of CBS
- Operations of CBS Branch
- Security and Controls at Data Centre and Branch

1.1 WHAT IS CORE BANKING SOLUTION?

Core Banking Solution (CBS) is centralized Banking Application software. It has several components which have been designed to meet the demands of the banking industry. Core Banking Solution is supported by advanced technology infrastructure. It has high standards of business functionality. These factors provide the banks a competitive edge.

There are different vendors in the market providing CBS. The software, (CBS) is developed by different software development companies like Infosys, TCS, Iflex Solutions etc., Each of the software has different names:

Name of the Vendor	:	Software
Infosys	:	Finacle
TCS	:	Quartz
Iflex Solutions	:	Flex Cube

Apart from the above, some institutions have developed the software in house.

The software resides in a Central application server which is located in the Central Office Data Centre. The application software is not available at the branch but can be accessed from the branches. Along with Data base servers and other servers, application server is located at the Central Data Centre.

All of the branches of the bank are connected to the Central Data Centre as shown in Fig.1.1.1

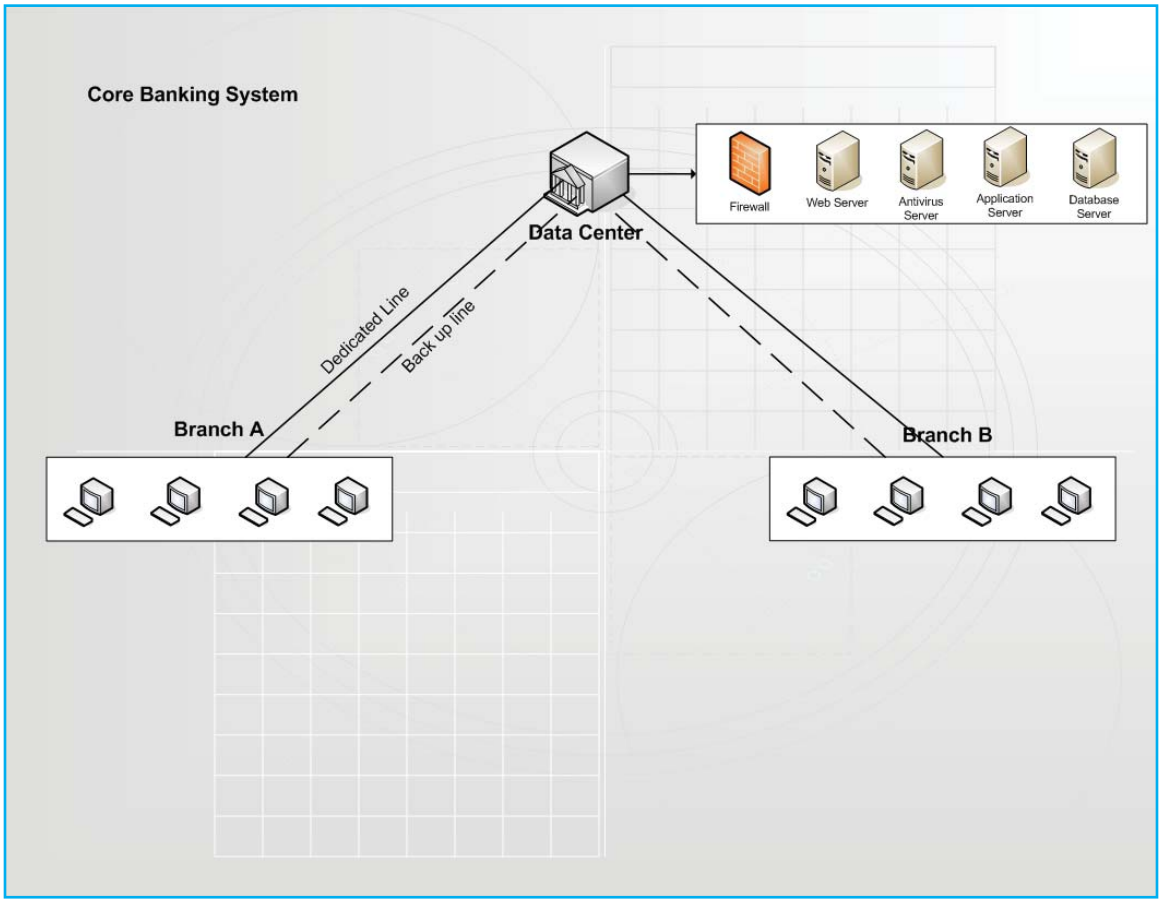


Fig. 1.1.1. Branches of the bank are connected to the Central Data Centre

Core Banking Solution brings significant benefits.

A customer is a customer of the bank and not only of the branch.

The CBS is capable of being implemented in stages.

Initially basic modules like Savings Account, Current Account, Fixed Deposits, Bills & Remittances, Loans and advances models implemented. Subsequently alternate delivery channels like ATM, Internet banking, RTGS/ NEFT, Mobile Banking, Treasury, Government Business etc., could be added.

As servers are on all 24 hours on all days, banking can be done any time and also from anywhere. Data base of customers is updated on line, e.g., amount withdrawn at ATM is deducted from the customer's balance almost instantly.

1.2 TECHNOLOGY BEHIND CORE BANKING SOLUTIONS

As already observed Core Banking describes the banking services provided by a group of networked bank branches.

As they are networked, customers can access their accounts and perform certain transactions from any of the bank's branches.

Broadly speaking, the customer is no longer a customer of the branch but a customer of the bank. Core banking solutions (CBS) is a combination of an application software and network devices. There is a Central Data Centre. Data Centre is a large data housing infrastructure that provides high band width access to its clients. The Data Centre houses many services, Networking devices, Firewalls and other related equipments. The figure below represents the technology and connectivity details in a very simple structure for the implementation of the CBS. The circled portion in the diagram would normally be in the Data Centre as shown in Fig.1.2.1

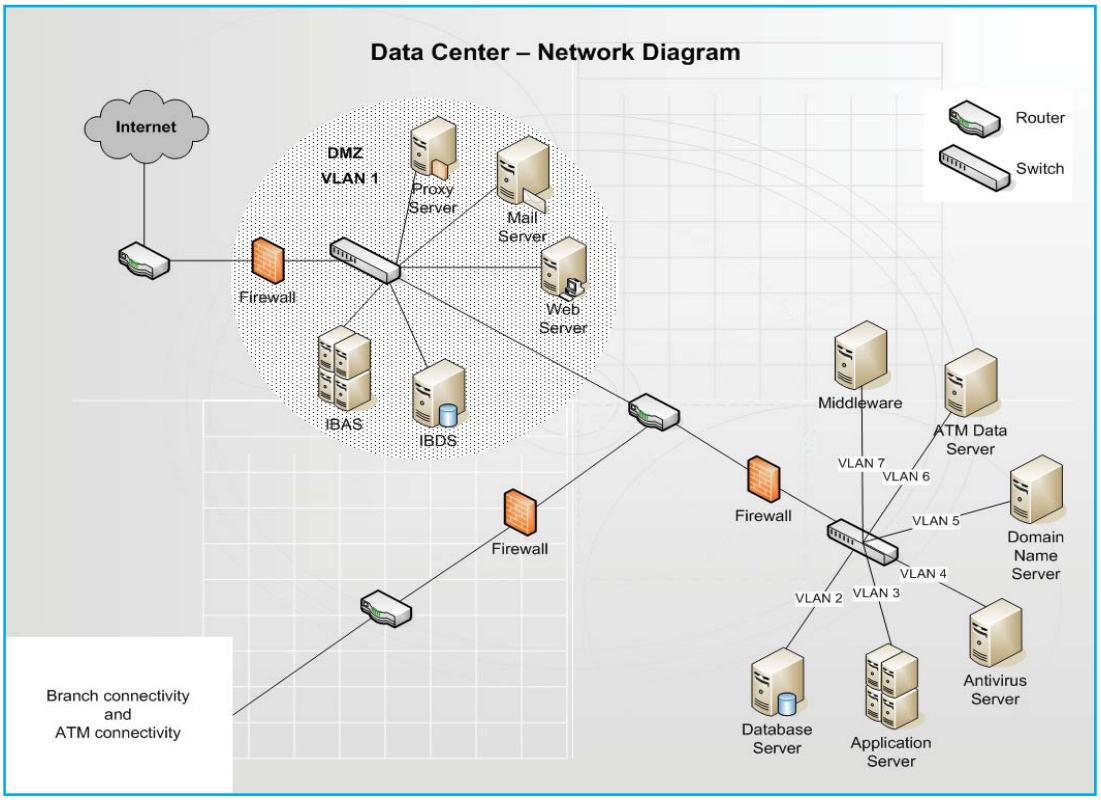


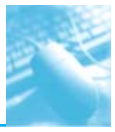
Fig. 1.2.1. CBS Network Diagram

The servers in the Data Centre could be many e.g., there are application servers, Data Base Servers, Web server, mail server, Report Generating Servers etc. It needs to be specifically emphasised that all the servers though placed in the same Data Centre are not in the same Local Area Network (LAN). Each of the servers are segregated using the concept of Virtual Local Area Network (VLAN). VLAN is a method of creating virtual networks within a physical network. Each virtual network thus created will act a a separate network. This concept has got distinct advantages:

Data communication between the 2 VLANs can be controlled as per business requirements.

Thus you will observe that in the diagram application server and data base servers are on two different VLANs (In the picture VLAN2 and VLAN3).

The various components of a core banking environment would be:



A Central Application Server that runs the core banking solutions (CBS). The application is centrally accessed by the branches. There are different core banking solutions available in the market like, Finacle developed by Infosys, Flexcube developed by I-Flex Solutions, Bankmate developed by the HCL Technologies, Quartz developed by TCS. There are other CBS software also some developed in-house by the bankers; others developed by other vendors.

Central Data Base Servers that store the data of the bank. It must be noted only this data base server that is centrally located stores the data for the bank which means that the data for all of the branches of the bank are stored in this central data base server.

Other infrastructure needed for internet banking and automated teller machine (ATM) operations.

Necessary infrastructure to provide security for stored data and data transferred across the network.

In the following paragraphs, we shall briefly discuss the various servers and their location and the purpose served.

At this juncture let us recapitulate the concept of a server. The server is a sophisticated computer that accepts service requests from different machines which are called clients. The requests are processed by the server and sent back to the clients. There are different types of servers as follows:

Application Server, Data Base Server, Anti Virus Server, Web Server, ATM Server, Internet Banking Application Server (IBAS),Internet Banking Data base Server, Proxy Server, Mail Server etc

Application server hosts the core banking application like Finacle, Flexcube, Quartz or Bankmate etc. This server has to be a powerful and robust system as it has to perform all the core banking operations. The branch does not have the entire application. It will have only a version which is called the "client version" of the application. The client version of the application is capable of only entering the data at the end point that is branches.

The validation is a complete process in the computer so that it ensures that data that is fed in conforms to certain prerequisite conditions e.g., if an operator keys in data for withdrawal of money , the account number of the customer would be entered by the operator naturally. But there would be a built in control so that further processing would be entertained only after the systems verifies that the account number which is now entered is already in the data base i.e., it is an existing customer. After the data is validated at the branch, it would be sent to the application server in the centralised data centre. The application server (which houses the banking software) after receiving the data performs necessary operations and updates the central data base etc., Customer "A" deposits Rs.10000/- is passed on to the data centre. The application server performs necessary operations and this updates the account of the customer "A" in the data base server. The customer may do some other operation in branch "Y". The process is validated at branch "Y" and the data is transmitted to the application software at the data centre. The results are updated in the data base server at the centralised data centre. Thus it would be observed that whatever operations a customer may do at any of the branches of the bank the accounting process being centralised at the centralised data centre is updated at the centralized data base e.

The application software which is in the application server is always to be a latest version as accepted after adequate testing; the application software is never static and would require some changes to be effected either due to any bugs discovered or a change in this process or any other justified reason. Such changes are never made directly into the live application server. These changes are made to a separate server called a test server. The programs are debugged and certified that the program is

now amended as required and performs as expected. The changed and latest application software will be moved into the application server under proper authority. Earlier version would be archived. The latest copy of the software would always have a back up copy.

Location

The application server would be placed in a trusted inside zone in a separate Virtual Local Area Network (VLAN) - please see diagram.

There is no direct access to the application server. The communication has to pass through a firewall, properly directed by a switch which is also located behind the firewall.

Data Base Server

The Data Base Server of the Bank, as already observed contains the entire data of the Bank. The data would consist of various accounts of the customers, as also certain master data e.g., master data are – base rates FD rates, the rate for loans, penalty leviable under different circumstances, etc., Application software would access the data base server. The data contained in the data base has to be very secure and no direct access would be permitted to prevent unauthorised changes. Strict discipline is followed regarding the maintenance of the data base server. There is a designated role for maintenance of the data base. This individual who performs the role is called the Data Base Administrator. His activities will also be monitored as all changes made would be recorded in a Log. Scrutiny of the log would disclose the type of activities and the effect of such activities. Security aspects of data base server are an audit concern. Apart from the normal application server, the Automated Teller Machine server (ATMS) and Internet Banking Application Server (IBAS) would also access the Data Base Server.

However, it would be only through VLAN. It must be noted that whatever be the operation that the customer has performed, etc., at the branch, through ATM, by Internet, mobile banking or any other alternate delivery channels his account at the Centralised Data Base would be updated.

Automated Teller Machines Server

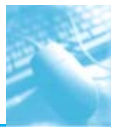
This server contains the details of ATM account holders. Soon after the facility of using the ATM is created by the Bank, the details of such customers are loaded on to the ATM server.

When the Central Data Base is busy with central end-of-day activities or for any other reason, the file containing the account balance of the customer is sent to the ATM switch. Such a file is called Positive Balance File (PBF). Till the central data base becomes accessible, the ATM transactions are passed and the balance available in the ATM server. Once the central data base server becomes accessible all the transactions that took place till such time as the central data base became un-accessible would be updated in the central data base. This ensures not only continuity of ATM operations but also ensures that the Central data base is always up-to-date.

The above process is applicable to stand alone ATM at the Branch level. As most of the ATM are attached to central network the control is through ATM SWITCH only.

Internet Banking Data Base Server

Just as in the case of ATM servers, where the details of all the account holders who have ATM facility are stored, the Internet banking data base server stores the user name, password of all the internet banking customers IBDS (Internet Banking Data Base Server) software stores the name and password of the entire internet banking customers (Please note that the ATM server does not hold



the PIN numbers of the ATM account holders). For further discussion, please refer to the chapter dealing with ATM. IBDS server also contains the details about the branch to which the customer belongs. The Internet Banking customer would first have to log into the bank's website. The next step would be to give the user name and password. The Internet Banking software which is stored in the IBAS (Internet Banking Application Server) authenticates the customer with the log in details stored in the IBDS. Authentication process as you know is a method by which the details provided by the customer are compared with the data already stored in the data server to make sure that the customer is genuine and has been provided with internet banking facility.

Location

The IBDS is located in a demilitarised zone. It has a separate VLAN that connects a proxy server, mail server, web server and IBAS.

Internet Banking

Internet Banking refers to banking transactions routed through the Internet. This facility permits registered customers of the bank to perform banking operations at any time of the day from any computer - now it may also be possible to do it from a cell phone.

No doubt, Internet Banking facilitates banking through the medium of internet. However, it also needs specialized software and hardware. The internet as you all know is a public network. Hence proper security features are built into the system to maintain confidentiality and integrity of the data that is being transferred through the internet.

Some Banks provide this facility automatically soon after a customer opens an account with them. Some others require a special request from the customer to provide this facility.

However, whatever be the method of providing internet facility, there is a process to be followed.

The main components of Internet banking system consist of Web Server, Internet Banking Application Server (IBAS), Internet Banking Data Base Server (IBDS), Middleware, and Central Data Base Server.

Anti Virus Software

In the pre Core Banking Solution scenario, when Total Branch Automation systems were in force updating the Anti Virus Software was yet another problem. As separate servers not connected to each other or to the Data Centre at the head office were in existence each of the server had to be updated with the latest version of the Anti-Virus Software separately

While in theory, it was agreed and presumed that all of the branches would have latest version of the Anti Virus Software, it was practically not so. As each one of the servers had to be updated manually with the latest version, the logistics proved to be inadequate with the result different versions of the Anti Virus Software were in existence in the different servers in the various branches.

In the Core Banking Solution as there is a Centralised Data Centre and also as there was a Centralised Data Base server, application server etc., the Anti Virus Software was also available only in the Centralised Data Centre. This copy of the Anti Virus Software was updated promptly and regularly at the Data Centre and pushed into all of the servers and in all the systems in the branches by push-pull method

Some Banks had, for back up purposes as also for business of the bank continuity planning had decided to have servers in the different branches. All the servers also were updated with the latest Anti Virus Software automatically every day as day beginning operations.

This process ensured that there was only one version of the Anti Virus Software and that too the latest one present in all of the bank's servers unlike in the TBA scenario.

1.3 COMPARISON OF TBA WITH CBS

Total Branch Automation System (TBA) was in existence before Core Banking Solution (CBS) was implemented. TBA itself was deemed a technology development compared to its predecessor ALPMS (Advanced Ledger Printing Machines).

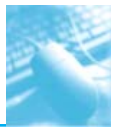
In the Total Branch Automation system each branch was performing the branch operations in totality at the respective branch. The final output was transmitted to the head office. The data was transmitted either on a CD or a Floppy. The information on this media was processed at the Central Office for consolidation of accounts and preparation of reports.

As each branch was self reliant in as much as all the information regarding the branch operations was available at the server located at the branch.

- The technology infrastructure at the branch was as follows:
- There would be a server which would be either in the Branch Manager's room or more commonly kept in a separate air conditioned enclosure with a separate entrance, so that entry to the server room can be restricted.
- At the most the Systems Administrator may be inside the cabin along with the server.
- There would be four or five nodes or more depending upon the need of the branch or the volume of transactions. Each of the nodes would be connected to the server.
- The server would have the application systems as also the data base.
- The bank as a whole would have one banking software which might have been developed in-house or purchased from an outside vendor. A copy of this software is loaded in each of the servers in all the branches of the bank.
- The server also hosts data base of the branch.
- The data base would have a master data, and all the details of the transactions entered into.
- The master data consists the data relating to standing information like the name, address of the customer interest payable on all Deposits. This would have the details of interest payable for various Deposits with different tenures eg. 8.5% pa, 9% pa 9% for two years and so on.
- Additional/ concessional interest for senior citizen, staff members, educational loan for girl child, various concessional rates during festive seasons etc.

Transactions of the customers would be stored account-wise, so that it would have the opening balance and the details of the transactions which have taken place.

The application software which is also residing in the server at the branch actually does the banking operations. Eg. A person operating a particular node (also called a client) (which is nothing but the front end machine from which the operations take place, enters the transactions. The customer might have come to withdraw Rs.10,000/-. The operator accesses the machine when he is prompted to give the user ID and password. Once he gives it correctly, a screen would pop up by which he would click the SB A/c and in the SB menu he would type the name of the customer as also the account number. He has now accessed to the specific account of the customer.



Next step that he would be doing would to be entering this transaction and request for withdrawal for the customer. In the example specified, he would be typing cash Rs.10,000/- in the appropriate fields. This command executed at the node end (client's end) is transmitted to the server through the communication channels (or net working cables).

At the server level the application accesses the data available of the customer in the data base and if there is balance available gives back the information. The transaction is put through.

Once the transaction is put through again this information is retransmitted to the server. The customer's data base is updated by the application and the customer's account would be suitably modified.

At this point of time, we are only discussing the process and not going into the details of the normal controls which are in place. Eg.

- If the customer does not have the required balance at his credit
- Is the withdrawal of cash a routine procedure which the person at the counter can authorise through controls built in the system whether the transaction can be entered by the person but would have to be authorised by an individual at a higher level say, the Accounts Officer. These procedures are built into the application software as part of built in controls of the software. This is known as maker-checker system or four-eye principle.

Similarly transactions relating to Current Accounts, Fixed Deposits, Loans, Foreign Exchange (where the branch is authorised to also deal with foreign exchange) would have to be dealt with by different nodes or same node and the data base of the branch is updated. By this process by the end of the day all the transactions which have taken place during the day have all been recorded and correct postings have been made to the respective accounts held in the database which resides in the server.

At the end of the day under the authority of the Branch Manager the Branch level Systems Administrator would perform End of Day operations (EOD).

The End of Day operations when completed would result in all the entries being posted and a final trial balance and other financial statements (including the complete ledger)(Opening Balance+Transactions leading to the Closing balance would be available).

The introduction of the Total Branch Automation hastened processing activities at the branch and also totally eased the time consuming End of Day Operations of preparing a tallied trial balance with all the ledger entries having been posted. A copy of the ledger is available in the system and this would be copied on a CD or a Floppy for outward transmission to the Head Office/ Central Office.

At the Head Office, the CDs and the floppies received from various branches would form a copy for them to prepare a consolidated ledger/ Balance sheet/ General Ledger

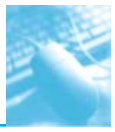
- The advantage of the TBA was that maintenance of manual ledgers and day books were dispensed with.
- At the end of the day, a neatly printed set of day books and ledgers with totals tallying (!) would be ready after last of the transactions are posted (in the initial stages due to technology snags or due to inadequate resources, the end of day operations were taking even 6-8 hours. However, after ironing out the teething problems, the time frame was considerably reduced.

Disadvantages

- As mentioned in the earlier paragraphs a copy of the software had to be loaded into each of the servers at various branches
- As we all know, the program require constant changes either due to bugs in the program or due to changes in the business process or for any other justifiable reasons.
- These changes are made at the central office (Computer Planning and Policy Department-CPPD). Copies of this program would have to be made effective at the branches.
- The methodology adopted for updating is that a copy of the programme would be taken on a CD or Floppy and passed over to a branch or personally carried by a member of the staff of the CCPD for updating the copy of the programme residing in the server of the branch. Sometimes it was also communicated through e-mail.
- While theoretically it seems simple, the problems that have been faced are with the need to change program often. There were different versions of the program available and operational at different branches of the bank. Version control mechanism was not effective.
- In addition to changes in programme master data regarding rates of Fixed Deposits, Loans, Penalties, etc., have to take place almost immediately in the entire bank at a single point of time. This was possible only by sending e-mails to the branches and instructing the Branch Managers to get the Systems Administrators of their respective branches to update the masters.
- The Branch Managers being busy with operations were not devoting time to personally ensure that these corrections are made properly. This resulted in a situation when modifications were made differently at different branches at different points of time.
- Also intentionally some 'mistakes' could be committed. This situation led to a great extent of chaotic condition of branch transactions at the head office and not to speak of suspense or sundry accounts created in each branch to ensure the trial balance tallied.

To get over this problematic situation, certain steps were taken to resolve the problems.

- For speedy resolution of problems at the branches, it was decided that source code would be made available at the regional office. All bugs would be dealt with at the regional level and corrected copies of the program would be given to the branches much earlier than it was possible earlier when all corrections were made only in the CPPD.
- The availability of the source code at the regional office and the different corrections being made by different people on different occasions lead to lack of control of programme changes and implementation of master data.
- The availability of source code at the different regional office itself was a matter of serious concern. The source code is the basic code which later becomes an object code. It is not possible easily to change a object code while the source code could be changed by anybody who knows the programming language.
- Apart from the serious operational problems and security concerns, there were certain other disadvantages like updation of anti-virus software.
- Scalability of the software was restricted. It wasn't possible to introduce further useful products like ATMs and Internet banking etc. It would have meant a great deal of patch work and it



will restrict new products. Already with various versions of program being available (and made necessary) in the total branch automation system, the programme was very weak with different versions having too many patches. To think of enhancing this to add further banking products like ATMs and Internet banking was bound to be impossible. ATM was introduced and work for the account holder of that branch only.

1.4 DATA CENTRE AND NETWORK CONNECTIVITY:

Data Centre houses all the main servers. They are:

1. Application Server
2. Database Server
3. ATM Server
4. Web Server
5. Antivirus Server
6. Internet Banking Application Server
7. Internet Banking Data Base Server
8. Proxy Server
9. Mail Server

Most of the servers are placed behind a firewall. The firewall is generally hardware and it plays the role of preventing unauthorized access. The servers though located in the same place will not be in the same Local Area Network (LAN). These servers are segregated by using the concept of Virtual Area Network (VLAN). VLAN has got its own security. The fig 1.4.1 below shows the network diagram at the data centre.

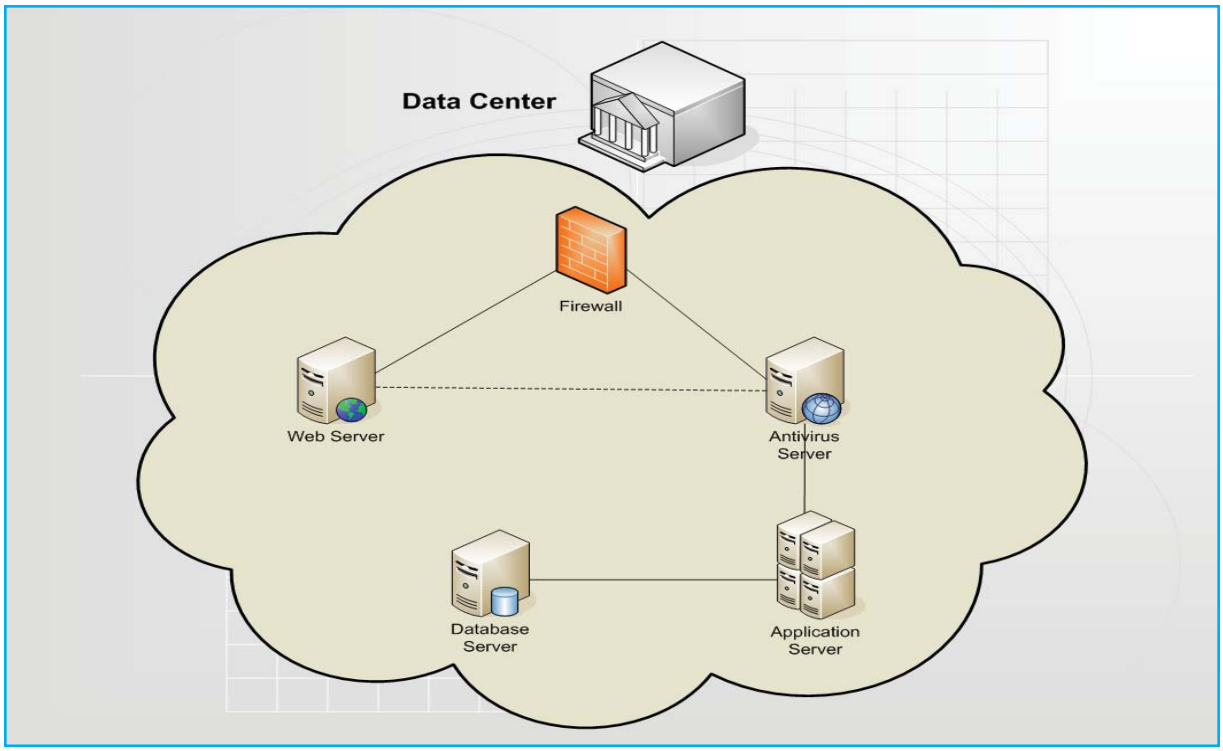


Fig. 1.4.1. Network Diagram at Data Center

Network connectivity

In a core banking concept all the systems of the bank are connected to the Central Office by means of a connectivity which may be either a leased line or a dial up line.

As the connectivity of the branch bank to the data centre is very critical arrangements was made for back up connectivity. In case the primary connectivity fails, there will be a fall back arrangement with a secondary line. There should be adequate band width capacity to deal with the volume of transactions that are expected to take place. When the band width is not adequate and the transaction load is higher, the system slows down and the efficiency also drops. Hence the banks should ensure that there is adequate band width to manage heavy load of transactions even during peak period like beginning of the month or end of the month/ year

Apart from the cables other important components of a network are devices like routers, switches and hubs. Routers enable data transmission over different networks. They are capable of making intelligent decisions to ensure data is transmitted across the network by using the best path. Switches have many ports that are connected to different systems. Switches facilitate data transmission with the network (this switch should not be confused with the ATM switch - discussed later). Virtual networks are capable of being connected only when devises are connected to a switch as shown in Fig 1.4.2.

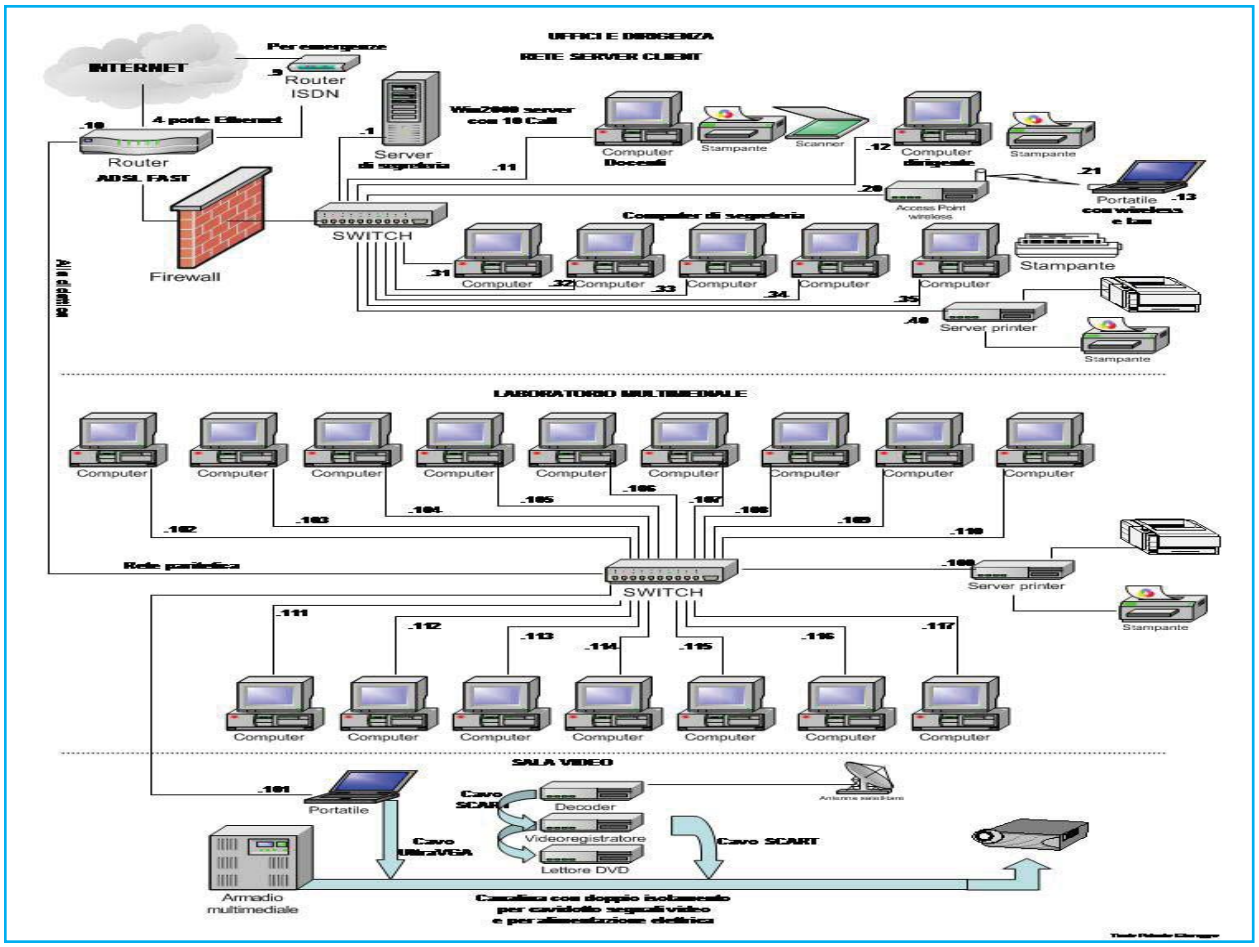


Fig. 1.4.2. Virtual Network Diagram

The picture above describes how the various servers are connected and where exactly the firewalls, routers and switches are placed. It will be observed that firewalls will always be placed whenever there is an access from outside the network.

Proxy Server

A Proxy server always acts in conjunction with a firewall. The Proxy Server provides network security by preventing malicious data from entering the network. In the network diagram, it will be noticed that the Proxy server is placed inside the demilitarized zone wherein the mail server, web server, internet banking application server, are placed.

Domain Controller

This is used for authentication. Access to a set of servers is controlled by the Domain Controller.

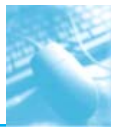
Network connectivity and security thereof plays a very important role in any organization especially in a core banking environment as the entire system is networked. The importance of network connectivity and its security can never be over emphasized. As dependence upon the network being available is crucial, adequate arrangements should be made for a fall back. The moment the primary network fails for any reason, the fall back arrangement comes into place due to the steps

already taken while establishing the connectivity. The network is vulnerable to "hacking". The hacking is a process of unauthorized entering a network. To prevent this hacking there have to be many controls in place. It is necessary to constantly monitor the network to ensure that there is no potential possibility of the vulnerability being exploited. All network traffic is required to be tested for vulnerability against hacking, phreaking, malware, spyware etc. There should be a specific team who will have the sole responsibility of constantly testing the network connectivity to ensure that it is secure. There are software tools available which would be utilized to assess the vulnerabilities. The tools when used would highlight any vulnerability discovered. The team in charge of maintaining the network would immediately take adequate steps that the weak points are strengthened. It is also possible that the network can be intruded. In any application and more so in banking applications vulnerability in the network or the possibility of a intrusion into the network are matters of grave concern. It is possible to use certain procedures so that any time an intrusion would be detected and prevented. A simplification of the concept could be that of installing a burglar alarm. Preventive controls have to be in place and it is the responsibility of the bankers to ensure the same. However, it is the duty of an auditor to verify and satisfy himself that the controls are in place and that competent and qualified people have verified and given satisfactory reports. Care should be taken to improve the security on ongoing basis as hackers are employing newer methodologies to attack network and stealing confidential information.

1.5 FUNCTIONS OF IT DEPARTMENT IN CBS ENVIRONMENT

As explained earlier, in core banking solution environment of Information Technology functions (IT functions) are centralised at the data centre. There are specific roles and responsibilities for different individuals like in all IT Departments. There are certain functions which are incompatible, which means that under no circumstance can one individual perform two different functions as those specific functions are sensitive. These functions have to be performed by two different individuals. This concept is similar to what we are aware of in a purchase function. The officer who is in charge of the purchase would not be the person who would be passing the goods. The person who passes the purchase invoice will be definitely different from these two. The rationale for the separation is that control will be compromised. This is known as segregation of duties and is very important in any computerized function. A brief description of the roles of different individuals in an IT Department is given below:

- **Security Administration:** It is advisable and necessary for all organizations including banking to have a security policy which is approved at the Board level. The officer in charge of the security administration is expected to understand the policies and procedures mentioned in the security policy. He should be able to assess the risks for non compliance. His duties would include deciding on access rules to data and other IT resources.
- There will be separate set of people who will be Issuing of user ID passwords and manage it. Monitoring the security architecture constantly with a view to ensuring that there are no weak points which can be exploited is the duty of security administrator. Security administrator should not have any access to transaction level data
- **System Administration:** This particular job is more sensitive. The Systems Administrator has the powers to create, modify and delete users in accessing the system. The individual is to be technically competent. He is also expected to have a proven record of integrity. His duties would briefly include the following:



- User creation
- User deletion
- Locating a branch code and providing connectivity to the branch
- Creation of new products
- Defining interest rates for deposit loans and other products.

- Be responsible for processing of end of day operations and beginning of day operations.
- Be responsible for introducing latest application of the program.
- **Data base administration:** As the very name indicates, the Data Base Administrator is the custodian of the bank's data. He is responsible for ensuring that access is given to the Central Data Base in a secure manner in line with business requirements. His responsibilities would include
  - Ensuring data integrity
  - Ensuring data availability
  - Ensuing security to access data
  - Importantly ensure recoverability of data in case of system failure
  - Maintaining size and volume of database and corresponding processes
- **Network Administration:** Networking, generally and more specifically in a core banking environment plays a very significant role. The Network Administrator has the following important responsibilities:
  - To place routers, switches and hubs at the appropriate places and ensure a secure network configuration.
  - Sensitive devises like firewalls and intrusion detection systems/ IPS need to be strategically placed to ensure security for the network.
  - At periodical intervals arrange for vulnerability assessment and penetration tests to take corrective action whenever these tests throw up weak points.
- **Librarian:** Normally we understand that the Librarian is in charge of maintaining the Library, issuing books and receiving them back. In a computerised environment, the Librarian has got similar functions excepting that instead of dealing with books, he will be dealing with software. As we are aware, the software, which is being developed and tested, would be clear as a complete product ready for use by the Project Leader. Such a program then moves from a test environment into the production environment. But there is an intermediary process by which the Project Leader hands over the finished product to the Librarian. The Librarian maintain records of the various versions of the program records all the various versions of the program just as we have different editions of a book and generally a later edition is expected to be important over the earlier one. Similarly, software may have different versions and it is extremely important to remember them and this number is referred to as the version number. The Librarian has the following responsibilities:
  - Moving the correct version of the software into production environment.

- Maintain detailed documentation of all receipts and issues of software.
- Keep a record of all licenses obtained for the usage of software.
- Be in charge of user manual and system manual

None of these groups of administrators should have access to the database having transaction data. Implementation of maker checker concept will ensure proper segregation of duties.

Changed Management Procedures

In the normal course, due to any change in the business process or upgradation of technology or due to program bugs discovered subsequent implementation changes are warranted in hardware, software and communication systems.

There needs to be a well documented procedure in place and a strict adherence to such procedure.

Changes to hardware and communication systems need to be entered in a register apart from a softcopy of the register being available on the system. The latest copy of the network program should always be available. These documents should always be maintained up to date incorporating all the changes and the dates when such changes have been incorporated.

Application Software

There needs to be a control on the various versions of software. At the stage of initial implementation of the software (for the first time software which has been debugged thoroughly moved from the test environment to the production environment) a specific version number should be provided e.g. CBS Version No: 1.1. There needs to be a document which contains details regarding the Version No. and date of implementation.

Thereafter for all subsequent procedures, there needs to be a strict procedure to be adhered to. The procedures would be as follows:

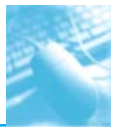
- There should be a specific request from an authorised person like the Manager of the user department. The request should be approved by the person in charge of the Systems Department.
- Changes to programs should necessarily be made in the test environment.
- After thoroughly debugging the program, the corrected program would be handed over to the Librarian.
- The Librarian would then give the next Version No. for the changed program, e.g. Version No: 1.2 (as compared to the previous Version No:1.1).
- The documentation would contain details of the changes made and the date when it was made.

Strict adherence to the procedures and technologies

The changes would ensure that the corrected latest version of the program alone is used. If such a procedure is not strictly adhered to, there is every possibility of an earlier version of the program being used, which would result in inaccurate processing.

Organization Structure of the IT Department

The standard for the organization structure for the IT Department is the same whether it is a banking environment or any other. The standards stipulate as follows:



- Production environment should be different from development environment.
- In the development environment all aspects of the program viz., functionality, built in controls, etc., will be tested by both the users as also the programmers. The programmers would test it first and then it would be provided to the user department for them to test it. This version is called the 'beta version'. Various types of tests like unit test, system test, and integration test conducted at this stage.
- After it has been tested by the users also, the Project Leader would hand over the software copy to the Librarian, who after completing the necessary documentation, transfers the program into the production environment. This is also known as user acceptance test (UAT)
- No one in the development and testing environments should have access to the production system.
- Production system is in a live environment and is accessible only by authorized users.
- Under no circumstances, should there be any connectivity between a test server and a production server.

As already discussed, there are certain incompatible functions which under no circumstances should be performed by the same individual. The Matrix provided below highlights the functions which are incompatible and those which are not.

	Help Desk	Database Admin.	Network Admin.	Security Admin.	Tape Librarian
Help Desk		X	X		X
Database Admin.	X		X		
Network Admin.	X	X			X
Security Admin.					X
Tape Librarian	X		X	X	

1.6 OPERATIONS OF CBS BRANCH

A branch in a Core Banking Solution environment is very different from a branch in a total branch automation system, as explained in detail earlier. Branches in a Core Banking Solution do not have independent operation in the sense that a copy of the application software or a copy of the data base of the customer is not separately available in the branch. Branches are connected to the central data centre, wherein there are separate servers housing the application software, data base as also antivirus software. Users at the branch have to be created by the System Administrator at the central data centre after due authorisation by the Branch Manager. Even a Branch Manager will not be able to create his own user access rights as everything is centralised.

At the Branch all operations that take place normally in an banking environment do take place; however, all master data are parameterised at the central office e.g., FD rates for various time periods, penalty, interest payable for premature closure, rates for different loans, interest rates applicable for staff members for loans and deposits, rates applicable to senior citizens etc., are to be decided centrally and parameterised at the central office. There is no possibility of any changes being made at the Branch as they have no rights to do so. There are certain account level parameters like preferential rates, addresses etc. can be controlled at branch level.

The various staff members operating at the branch have been given access rights by creating a User ID by the Central Office and also providing an initial password which necessarily will have to be changed by the individual employees soon after they make the initial log in.

There would be a register maintained at the branches, where in each of the individual would have acknowledged their user ID and the recommended format for the register would be as follows:

1. Name of the Employee	2. User ID	3. When created	4. When deactivated	5. Signature of the employee

Maintenance of this register is of utmost importance as it acts as evidence that the respective employees have acknowledged their user IDs. All the transactions performed during the period from the time the account was created to the time it was deactivated would be attributable to the employee in view of the accountability being established, employees would be extremely careful not to disclose their password or share it with others. The minimum level of controls which needs to be in operation would include the following:

- A branch should have an extract of the bank's security policy as applicable to it.
- There should be some evidence of having created awareness amongst the employees regarding the existence of the security policy of the bank.
- There should be a well written procedure in place to record and document all incidents of security lapses.
- There should be regular procedures to create basic IT security awareness amongst employees.

Access Control Procedures

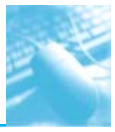
- The system should prompt for change of password during the first log in.
- There should be a maximum number (usually 3) of failed log in attempts. The rationale for this requirement is to prevent multiple guesses being made by unauthorized user
- There should be a procedure for reviving such accounts which should have been deactivated.
- All USB ports, the CD Rom drives should all be disabled. This is necessary to both prevent unauthorised data or software being loaded and also to prevent any leakage of data and information. If this facility is not strictly adhered to, the possibility of virus being introduced into the system is very high & there is a chance of data loss/ leakage to unauthorized user.

Server related procedures

Generally there should be no servers available at the branch. However in some instances a local server is installed to get over slow connectivity problems. Under such circumstances, the local server serves as a temporary storage. The discipline connected with the local server is as important as any server and there should be a specially designated branch system administrator who would be having a specific password to access the server. A copy of the password should be kept in a sealed cover under the control of the Branch Manager, so as to enable him to utilize the same should the system administrator of the branch be not available on any day.

Physical and environmental controls

Moisture and temperature in the room where the server is located should be under control. There should be no inflammable material stored in the server room. In some instances, it is not uncommon



to find bundles of paper and some thermo cool boxes being stored safely in the server room which need to be reused immediately

There should be a fire extinguisher in the room, which should always be in an active condition with the refills of gas being done at regular intervals or there should be other mechanized process for extinguishing the fire.

Network related procedures

Network devises like the router, switches and hubs should be secured. Unused routers, switches and hubs should be protected, if not they could be misused and there could be unauthorised use of handling the system but also leakage of important data. All network cables should also be protected properly. There are instances when these cables are running outside the building without being properly encased. Unprotected cables have the potential for being hacked.

ATMs being attached to the Branches

- ATM cards which are awaiting to be handed over to the customers should be secured with a lock and key.
- There should be regular reconciliation procedures for the stock of ATM cards.
- There should be procedures to update core banking solutions with details of cards issued to the customers. This would prevent the possibility of usage of the card before it is issued to the customers.
- Frauds do occur when ATM cards and Pin mailers are not kept separately & securely. Especially the ATM cards should be with one officer and the Pin Mailer should be with another officer. Under no circumstances both the ATM cards and Pin Mailers are kept together. When they are kept together any employee can pick up the ATM card and a pin mailer with similar address and try using them fraudulently at the ATM. Such occurrences of fraud have been reported several times.
- When ATMs are attached to the branch, there should be procedures for loading cash, recording and reconciliation of cash. The master key of the ATM should be under dual control. The ATM journal rolls should be stored safely in the branch as they form an important document for reconciliation purposes & for detecting any unauthorized use/ transaction
- There should be strict procedures for dealing with swallowed card.
- There should be clear procedures for dealing with cash which is in the reject bin.

Business Continuity Planning and Disaster Recovery Planning

- There should be a document detailing the Disaster Recovery procedures as well as Business Continuity Planning.
- There should be evidence of having created awareness amongst the employees for action to be taken for DRP and BCP.
- There should be evidence of periodic drills having taken place. This would act as a proactive control.
- There should be clear documentation and alternate connectivity being established by the banks with the data centre in case of their being a brake down in the primary connectivity.

1.7 SECURITY AND CONTROLS AT THE DATA CENTRE AND BRANCHES

Branch

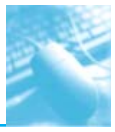
Branches are not generally in a position to generate new reports locally. Only those already provided in the application would be generated at the data centre. In some core banking environments at the data centre, there is a server normally referred to as "Report Generating Server". The CBS application generates these reports and stores it in the report generation server. The branches have access to the report generation server and would be in a position to down load the required reports. There is also a practice of a folder being created for each branch in the report generation server. Evaluation of security controls are as already mentioned very different from that in a total branch automation (TBA) environment. In all the reports that may be required for audit is available in the branch for 'view' & print only.. Given below is a brief check list for evaluation of security and controls of a branch in the CBS environment. The various aspects which would be covered are as follows:

1. Information Security Policy
2. Access Control Procedures
3. Procedures connected with branch servers
4. Physical and environmental control for the servers
5. Network & Communication control
6. Limited verification of applications
7. Operations connected with ATM/ Internet Banking
8. Business Continuity Plan
9. Change control procedures
10. Others

In the core Banking scenario, auditors may be given specific access through which he can download the data as per his requirement and export to a excel sheet for further analysis. In certain Bank, various other analytical reports are available from data ware house system which takes the data dump from core banking solution and generates various intelligent reports as per requirements.

Information Security Policy

- Does the Bank have a Security Policy? Is a copy available at the Branch? If the whole copy is not available at least those relating to the Branch Operations are available? Any job-cards available?
- Are the employees aware of the existence of the security policy, its contents and the expectation of the management regarding their compliance?
- Is there any record maintained of any security lapses? Are security incidents reported?
- Are there guidelines available at the branch for reporting such incidents of security handling?



Access Control Procedures

Password Management:

- Is there a procedure built into the system by which change of password is enforced before password lapses?
- Does the system ensure that during the first log in the password is changed?
- The original password given is known to the system administrator as he has allotted it. Hence it is absolutely essential that at the first log in using the default password, the process of creating a fresh password should be completed. If this process is not in place the sanctity of having a password is lost.
- Verify the procedure adopted for communicating the user ID to new employees. This is generally done by e-mail. But it is necessary to have a hard copy and the signature of the employee obtained on the same.
- Is there a procedure in place to ensure that the account gets locked if wrong password is used for say three times? This is to ensure that an unauthorised person would not indulge in accessing the password.
- Verify the procedure in place to revive locked accounts. The locked accounts should be capable to being unlocked only by the system administrator at the data centre. Or a centralized process is available to unlock by the same user after authenticating himself via previously set question answer.

User ID Register

There should be an user ID register (a hard copy) which should contain details of when the user ID was given and when it was disabled. This information should be signed by the employee. Obtaining the employee's signature alone establishes accountability and also the time period for which he has been using the user ID. In the absence of such conclusive evidence established, fool proof evidence of accountability in a case of fraud or any other unauthorised activity would be difficult.

Session Activity

Is there a procedure to ensure that a system is not open after a certain period of time? Generally the session will not be allowed to be idle for more than ten minutes. This is to ensure that when the session is kept open unauthorised usage will not be made. The users are expected to log off if they are going to be away from their seats for more than a reasonable length of time.

Disabling the drives

All external drives like floppy drive, CD Rom drives or USB ports should be disabled in all the systems at the branch. If this procedure is not followed, it is possible both to insert and leak unauthorised information. More importantly also virus may be introduced.

Server related procedures

In a core banking solution as already mentioned all servers are hosted only at the central data centre. However, in some cases, for the purpose of operational efficiency, a bank may decide to have a server installed at the branch. It should be ensured that the contents of the servers are verified. At the most, it would be acting as an intermediary server to solve connectivity problems. It is not uncommon to find that when the traffic is slow, band width seems insufficient and processing slows down. Some

banks have a server at the branch for this purpose. In some other cases, at the time of beginning of the day, the opening balances of the branches are loaded so that if connectivity is lost with the data centre, the bank will be able to continue with the operations till such time such connectivity is reestablished.

It should be verified whether there is a specifically designated systems administrator for the server at the branch. His password should be available in a sealed envelope which can be used by the Branch Manager in his absence.

Physical and environmental controls

- Ensure that there is some automated system installed to monitor humidity and temperature in the server room.
- Are there procedures in place to restrict entry only to authorised persons to the server room. Whether multi factor authentications are in place?
- Is there a register being maintained where the name of the person and his signature and time of entry to the server room are entered.

Network

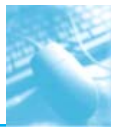
- Verify whether all network cables are protected adequately. In some instances, the network cables may be running on the external walls of the building. In such circumstances potential for intrusion is very high and communication passing through those cables is insecure.
- Verify that there are no unused ports in router, hubs and switches.
- Unused ports should not be available or if available should be adequately protected. If they are not adequately protected an unauthorised node could be connected.

Application level verification

- Application needs to be decided to verify whether it permits back dated entries.
- Does the system have built in control which ensures that significant parameters like interest on deposits, interest on loan are range bound.
- Testing this aspect would ensure that unreasonable parameterization by mistake or intentionally would get introduced.
- Verify whether application logs are generated. This needs to be comprehensive enough to provide information regarding user ID for each of the transactions. It should also provide information as to be able to identify node/machine from each transaction was generated.

Process regarding to ATM Operations attached to the Branch

- Are the procedures for storing the ATM cards secure?
- Are there procedures in place to reconcile the physical stock of ATM cards, eg., a register should be maintained regarding cards received and cards issued to customers. Cards returned by customers and balance on hand.
- Is the branch received pin mailers. Generally the mailers should be sent by secure methods like reputed couriers directly to the customer. Should the Pin mailer and the ATM card be received at the branch and retained their security is a matter of concern. The possibility of matching the



pin mailer with the corresponding card by looking at the address could lead to unauthorised and fraudulent transactions.

- Are there procedures in place to ensure that the pin mailers and cards are under the safe custody of two different officers?
- Procedures for returned PIN mailer & cards to be verified invariably.
- Are there procedures in place for updating the main core banking system with the details of the cards issued to the customers?
- It is necessary that this procedure should always be in a set of updatedness as otherwise there is a possibility of a customer being denied ATM access as the details of his card are not available in the main data base.

Operations of ATM that are attached to the branch itself

- Verify whether there are procedures for cash loading, recording of cash transactions and a final reconciliation of the balance.
- Verify whether the ATM master key is under dual control. This is extremely important as encryption process depends upon the security procedure adopted. The encryption key is divided into two parts and each of the officers would be able to load only one half. Hence, if the dual control is effective no one person will know the encryption key.
- Verify the procedures for storing the ATM journals. The ATM journals play a very significant role in reconciling the transactions which have taken place in the ATM.
- Verify the procedures which are in place for dealing with swallowed cards. Swallowed cards should be kept in safe custody and after proper scrutiny they have to be returned to the established owners of the cards or returned safely to the central office.
- Verify the procedures for reconciling the cash in the reject bin.

CHAPTER 2

CBS INTERFACES THEIR FUNCTIONALITY AND CONTROLS

LEARNING OBJECTIVES

- Automated Teller Machine (ATM)
- Internet Banking / e-banking
- Real Time Gross Settlement (RTGS)
- Cash Management System (CMS)

2.1 AUTOMATED TELLER MACHINE

Automated Teller Machine (ATM) is a computerised telecommunication devise. Usage of this facility dispenses with the need for a bank teller. This facility provides a customer to access financial transactions in a public place. ATMs may be installed within the branches, away from the branches and at shopping malls also.

The facility of ATMs provided by one bank may be utilised by ATM card holders of other banks also, who would have entered into an agreement to share such facility.

ATM Card

The ATM card has a magnetic strip. The card contains an unique number and some other security information apart from date of expiry of the card. The ATM card is issued only to existing customers of the bank. The customer has to fill up an application form and submit the filled in form to the branch to which he belongs. The concerned Branch Manager recommends and authorises the issue of an ATM card by forwarding the application to the Central Office which deals with the issue of ATM cards.

In view of the severe competition now almost all the banks provide to their customers soon after they open an account with the facility to perform internet banking and possess an ATM Card.

Procedure for issuing ATM Cards

At the Central Office, there is a specifically designated computer system which has specific software. The application form received from the customer is the input for the process and the output consists of a file containing data for the preparation of a ATM card. The software checks whether the customer details provided in the application tally with the data contained in the Central Data Base of the Core Banking Solution. Only after the details tally, the output file is generated. The Personal Identification

Number (PIN) is generated by the software and directly sent to equipment for printing the Pin Mailer. It is to be noted that the PIN generated is not stored in the memory of any machine.

As a concurrent process, a natural PIN is generated and stored in the data base of the ATM switch.

ATM switch should not be confused with normal switches.

ATM switch is a computer with a server attached to it. Data base resides on the server.

Natural Pin

There are different methods of generating a natural PIN. The natural PIN is a number. One of the methods adopted is to encrypt the card number. After encryption, the encrypted value of the card number is obtained. This encrypted value is decimalized which in turn will produce a number with several digits. The first four digits of the above number is called natural PIN. The natural PIN (the first four digits of the above mentioned number) is deducted from the PIN value. As mentioned in the earlier paragraphs, the PIN number is generated even while preparing a file for preparation of ATM Cards. The value of the natural PIN is deducted from the PIN value which gives the offset value.

PIN No (-) Natural Pin (=) offset value.

It will thus be observed that every time the value of the natural PIN is added to the offset value, the PIN of the customer is generated. It is important to note that the PIN number of the ATM customer is not stored in any ATM machine or ATM switch. Only the offset value is stored and only the customer knows the PIN number. The PIN is communicated to the customer by means of delivery of a cover which contains the PIN mailer. As we all know neither the PIN mailer nor the ATM card is sent through ordinary mail but only through trusted couriers. It is a good practice to send the ATM cards to the concerned branches and the PIN mailer by courier to the customer directly.

ATM Operations

The ATM generally performs the following functions:

(a) Cash Withdrawal

(b) Balance Inquiry

(c) Registering requests for cheque book

(d) Changing of PIN number

A sample of the ATM network would be as shown in the fig 2.1.1 below:

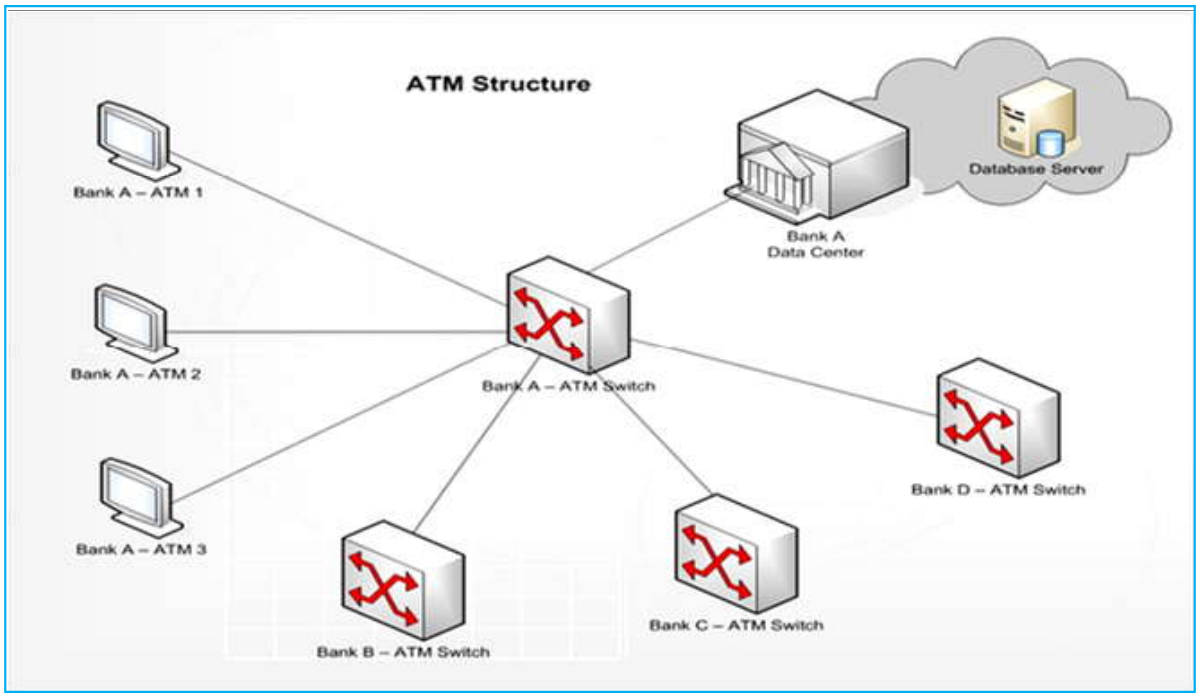


Fig. 2.1.1. ATM Network Structure

All the ATMs of a particular bank are connected to an ATM switch of the bank and the ATM switch in turn is connected to the server of the bank by means of internet connection. The ATM switch is not like other switches; but it is a server. There is an operating system residing in the server.

ATMs may also be connected to the switch by means of a leased line or dial uip line.

A single data base of all the customers of the bank resides in the Central Data Base at the Data Centre of the Bank. The data base itself resides in the data base server to the Data Centre.

Functioning of the ATM

- The customer swipes his ATM card and information provided in the magnetic strip is read by the machine.
- The customer has to key in his Personal Identification Number (PIN), which he has received by means of PIN mailer sent by the bank
- The PIN entered is immediately encrypted by the machine called the PIN machine. Sometimes this process is also achieved by means of the software which resides in the ATM server. The encryption may be done by means of a hardware or software. When it is done by the hardware, there is a hardware security model (HSM); if this is done by software, there is a Software Security Model (SSM). HSM or SSM encrypts the PIN entered by the customer by means of an encryption algorithm. This algorithm is loaded into the machine by the officers of the bank. As it is necessary to ensure security, the loading process is done under dual control by two officers each loading one half of algorithm.
- When the account number and PIN provided by the customer tally with the data available at the data base of the switch and PIN generated by the PIN machine the customer is authenticated; it means that the customer has been recognized as a genuine customer of the Bank.

- It will be observed that loss of ATM card alone is not a matter of concern such as losing both the ATM card and the PIN information
- Once the customer is authenticated the process requested by the customer is initiated, e.g., the customer has asked for cash withdrawal. This request for withdrawal of cash is passed on to the data base of the bank, which is available in the data base server at the central data base. At this juncture, the system verifies whether the customer has adequate balance to enable him to withdraw the cash required. Once it is ascertained that adequate balance is available, the ATM switch which receives the information authorises dispensation of cash required at the ATM machine.
- The activity of the cash disposal is facilitated by the ATM switch. The cash is then picked up by the customer.
- After the cash has been dispensed and the customer has picked up the cash, the ATM switch communicates with the Central Data Base server so that the cash withdrawal is recorded and the balance is accordingly reduced.

At the ATM: Cash journal and the ATM log are generated recording the process which has taken place. There are also electronic journals which are generated at the ATM. When ATMs are located in remote places, the information with the electronic journal can be retrieved by a process called as Electronic Journal Pulling.

- As we all know, there are arrangements between banks by which ATM card of one bank can be processed at the ATM kiosk of another bank. This process is possible within the banks which have entered into an agreement to this effect. The process that follows when the ATM card of a different bank is swiped at the ATM kiosk is slightly different. As the ATM card of another bank is swiped, the information regarding the bank and the customer number are available to the ATM. The information so obtained is directed to the ATM switch of the other bank. The process thereafter is similar to the process discussed in the above paragraphs.
- It is possible that a customer did not or could not collect the cash dispensed by the cash dispenser. In such a case, the cash dispensed would be collected in a secure tray for collecting rejected cash. Also the fact that cash was not collected would be reported by the ATM to the switch. The switch in turn would request the host computer for reversal of entry. This would result in the original debit entry passed at the central data base being reversed so that the customer is not debited with an amount he did not or could not collect.
- The switch and the host computer log all the events, thus facilitating reconciliation of cash and entries.

In view of the facility of the usage of ATM card of one bank in another bank's ATM kiosk there are certain other factors of importance. The cash is dispensed by one bank on behalf of another bank. As this operation takes place in all the banks, there is a process of reconciling these cash transactions, so that the respective banks are reimbursed with the net amount due to them.

Verification of the PIN

The customer enters his PIN and there is a process which takes place before the PIN is accepted and authentic by the machine. The various steps are as follows:

1. The customer inserts the card and thereafter types the PIN.

2. The encrypted PIN is sent to the ATM switch.
3. The details of ATM card issued are already in the data base and when the ATM card is inserted the machine verified to see whether the number is in the data base and satisfies itself of its existence.
4. From the card number natural PIN is generated. As already discussed natural PIN is generated by decimalizing the encrypted value of the card and considering only the first four digits represent the natural PIN.
5. (a) The difference between the actual Pin and the natural PIN is stored in the ATM switch as an initial step. Subsequently whenever the customer inserts his ATM and keys his PIN in the machine, the correctness of the PIN is verified by the system by adopting a process as described below: The system has stored the offset value (offset value is the Difference between the actual PIN and the natural PIN)

   (b) When the card is inserted, the card number is encrypted by the HSM or the SSM. The encrypted value is decimalized and the natural PIN is obtained (which is the first four digits of the value obtained by encrypting the card number and decimalizing the same).
6. This value of the natural PIN obtained is added to the offset value available already in the system. At this stage, the relevant PIN is generated within the system.
7. The generated PIN as described above is compared with the PIN typed by the customer; if they tally the customer is authenticated.

Knowing the PIN alone will not facilitate a person to access the ATM facility. It is a combined effect of the ATM card and the PIN which permits access to the ATM.

Change of PIN

Just as there is a facility for an user of a computer to change his password, it is admissible and possible for an ATM card user also to change his PIN. This may be done for security reasons. The process of changing the PIN is as follows:

On the key pad at the ATM, there is a key 'Change No.' when this key is pressed the ATM will ask for the old PIN. The customer is to key in his old number and then only key in the new PIN number he proposes to have. By making use of the process of generating the natural PIN and summing it up with the card number, the ATM will be able to arrive at the old number and satisfy itself that the person who wants to change his PIN is an existing customer, who has been given an ATM facility. After thus satisfying, the machine permits the customer to enter his new PIN. As the natural PIN is already available the new offset value is computed and stored. The old offset value is erased. For all future operations making use of the natural PIN and the offset value available, it generates a new PIN with which it able to compare the PIN keyed in by the customer. It is important to note that nowhere in the system is the PIN stored. There is only a process of computing PIN corresponding to the ATM card inserted.

Normal operational problems faced with the ATMs

- Cash may not be sufficient. There may be a sudden overdraw of cash contrary to expectations.
- The journal paper roll might have been exhausted and a refill may not have been placed.
- If the network connection is lost or there is some other operational problem, the ATMs may not function.

- There is a monitoring facility available with the Bank by which information is available as to which ATM has stopped for what reason.

It is possible that a card holder by mistake may key in a wrong PIN. The ATM machine will not give him right to access. Generally all ATMs permit only three chances to commit mistakes and should a fourth attempt be made, the card will be rejected.

It is also possible that the card may be stolen. The owner of the card might have instructed the bank to hot list it. Hot listing is similar to countermanding of a cheque. If a card which is hot listed is inserted into an ATM, the machine will swallow the card thus preventing the usage of the card.

Evaluation of Control of ATM Operations

As already discussed, there are various processes in ATM operations and it is absolutely essential to evaluate the adequacy of controls in each of these areas. In the paragraphs to follow, the controls which have to be in place in the different operations are discussed. The different heads of operations are:

1. Card and Pin generation
2. Method of dealing with surrendered and captured cards
3. Security of the PIN
4. Control over cash
5. Minimum records to be maintained for transactions
6. Method of dealing with lost and stolen cards
7. ATM switch operations

For evaluating adequacy of controls one should be aware of what controls need to be in place.

Card and Pin generation

- There should be separate departments and members of staff for card and pin generation.
- The pin mailer tape should have card and account number
- There should be reconciliation procedure for the number of PIN mailer and cards produced.
- This should take into account not only the number of cards and pins produced but also those spoiled.
- There should be adequate security procedures for
  - (a) Access to the building
  - (b) Stock of blank cards
  - (c) Stock of live cards and pin mailers
- The pins on the tape should be in an encrypted state.
- Live cards and pin mailers should be dispatched separately from different locations eg.,
  - (a) ATM card should be dispatched from the Branch and
  - (b) Pin mailer should be dispatched from the Central Office.

- There should be proper records for all delivered cards.
- The returned cards and returned pin mailers should be with two different officers. This procedure is extremely important to avoid any fraud being committed by a person picking up a card and the corresponding pin mailer. This could be easily done with reference to the address being the same on both.

Surrendered and Captured Cards

- There should be clear documentation regarding surrendered and captured cards.
- There should be documentation for issuing replacement for cards and pin numbers.
- There should be procedures for making the captured cards ineffective either by the card holder or by the bank.
- Instructions should be in place to inform the customer that the pin mailer should not be returned to the bank.
- There should be a register maintained for all surrendered cards. The captured cards in the bin should be opened in the presence of two officers and details thereof entered in a register duly signed by both of them.
- The journal roll at the ATM would also be recording details of the captured cards. The captured cards should be removed on a regular basis and reconciled with the journal roll.
- The host computer at the data centre should be producing a report on the captured cards.
- There should be clear procedures available for reissue of cards or change of the PIN numbers.
- There should be a control procedure by which the ATM swallows the customer's card after the customer has made three failed attempts to key in the correct PIN number.

Security of the PIN

There should be a procedure in place to stop the card operation, when the card holder reports to the bank that his PIN has been compromised.

The customer should be advised never to disclose the PIN number to any other third party including the Police.

- There should be procedures in place for generating a new PIN number on a timely basis should the PIN be lost or stolen.
- PIN number should be held in data files only in a encrypted from.
- PIN offsets also should always be encrypted.
- There should be a process in place for either hardware encryption or software encryption (HSM - Hardware Security Model and SSM - Software Security Model).
- There should be procedures in place by which all work and storage areas used for PIN encryption are zeroized after each calculation.
- There should be no hard copy available in the system of records of PIN produced.

Control over Cash

- There should be documented procedures for cash control and balancing process.

- Data roll should automatically record all insertion and withdrawal of cassettes.
- There should be records indicating amount of cash inserted into each cassette.
- The Bank staff should reconcile duly the following:
  (a) Cash inserted
  (b) Cash dispensed
  (c) Cash remaining
  (d) Miffed notes
- There should be a procedure to monitor all discrepancies reported.
- Individual responsibility for the reconciliation should naturally be a person different from the person responsible for the maintenance of cash.
- There should be a procedure to ensure that wrong denomination notes are not inserted into the cassettes.
- Daily balancing process should ensure that:
  (a) The currency deposited and dispensed should agree with the ATM cumulative total;
  (b) The total of the deposit and withdrawal transactions generated by ATM should also be logged by the host computer and the branch System.

Minimum records to be maintained for transactions

- There should be a journal roll fitted to each ATM. The journal roll records all events at the ATM and hence is of great importance.
- Hard copies of the journal should be preserved securely.
- There should be a built-in procedure to have a soft copy of the journal.
- The soft copy is also called an 'Electronic Journal'. It should not be possible to modify the soft copy. The soft copy should be stored securely.
- Only the authorised key holders should be permitted to make weekly check of the journal roll machine record. Verification by the of the record would disclose if there had been any unauthorised opening of the ATM or any operation removal of cassettes.

Standard methods of dealing with Lost and Stolen Cards

- There should be documented procedures to be followed to deal with stolen /lost cards.
- An up-to-date file containing all details of reported lost and stolen cards should be available.
- The access to this file should be restricted.
- There should be a facility to immediately identify when a stolen or lost card is used.
- There should be a trigger to reject the transaction or capture the card.
- Even when instructions to stop usage of ATM cards are given verbally there should be provision to take action against the same.
- There should be a written notification from the card holder about his card being stolen or lost and then only a replacement card issued.

- There should be a policy in line with legal provisions relating to the liability for withdrawals made prior to and after notification of a card being stolen or lost.
- All reports regarding lost and stolen cards should be retained for a reasonable length of time,

ATM Switch Operations

As already mentioned ATM switch consists of a computer with a server attached to the same. Details of the ATM card holders is available at the data base, The details would include

(a) Card No. and corresponding offset value (offset value has already been discussed earlier)

(b) Details of hot listed cards

(c) Details of surrendered cards and

(d) Account balance of customers. (This account balance is also called positive balance file - PBF. This is made available at the ATM switch. Even when the ATM is offline, the balance of the customer is available.

The important control points to be reviewed for audit purposes would include the following:

- There should be a Security Guard as also a CCTV (Close Circuit Camera)
- A register should be maintained at the entry point.
- The server has an operating system. The settings of the operating system need to be reviewed to ensure it is in line with the best practices.
- Only the Systems Administrator and none else capable should be capable to access to the operating system.
- The ADMIN Password should be kept secure.
- The application software, which is in the switch, has details of the maximum number of withdrawals per day, the limit for the withdrawal, number of failed attempts etc., these are parameterized.
- The procedure for configuration the parameter should be reviewed.
- Only an authorised person should be capable of making these modifications.
- Procedures in place for key storage should be reviewed. Security of key used for encryption and decryption purposes should be evaluated.
- Review of procedure for hot listing of ATM cards needs to be reviewed.
- Examination of the types of logs that are generated and review of such logs is important.
- When there is an agreement with other bank's for usage of their ATMs such agreement should be reviewed especially with reference to customer claims for "money not received but account debited".
- Very importantly, review should be undertaken of procedures in place to deal with another bank / branch reconciliation.
- Any undue delay in reconciling these may give rise to mushrooming of unauthorised entries getting masked in the account

2.2 INTERNET BANKING

Internet Banking refers to banking transactions routed through the Internet. This facility permits registered customers of the bank to perform banking operations at any time of the day from any computer - now it may also be possible to do it from a cell phone.

No doubt, Internet Banking facilitates banking through the medium of internet. However, it also needs specialized software and hardware. The internet as you all know is a public network. Hence proper security features are built into the system to maintain confidentiality and integrity of the data that is being transferred through the internet.

Some Banks provide this facility automatically soon after a customer opens an account with them. Some others require a special request from the customer to provide this facility.

However, whatever be the method of providing internet facility, there is a process to be followed.

Process

The main components of Internet banking system consist of Web Server, Internet Banking Application Server (IBAS), Internet Banking Data Base Server (IBDS), Middleware, and Central Data Base Server.

We give below a broad Data flow diagram describing the Internet Banking Process.:

<table>
<tr><td rowspan="2">Customer

Customer using a browser such as Internet Explorer to access the Web</td><td>Web Server & Web host</td><td>IBAS

Internet Banking application Server</td><td>IBDS

Internet Banking Database Server</td><td>Middleware</td><td>Central Database Server

All data to and from the Core Database server is scanned by Firewall</td></tr>
<tr><td colspan="3">De-Militarized Zone (DMZ)</td><td colspan="2">Trusted Inside Zone</td></tr>
</table>

Web host is a system that has an operating system and runs the services from the Web server. All data to and from the Web server are scanned by the Firewall as shown in Fig 2.2.1(A) and Fig 2.2.1(B)

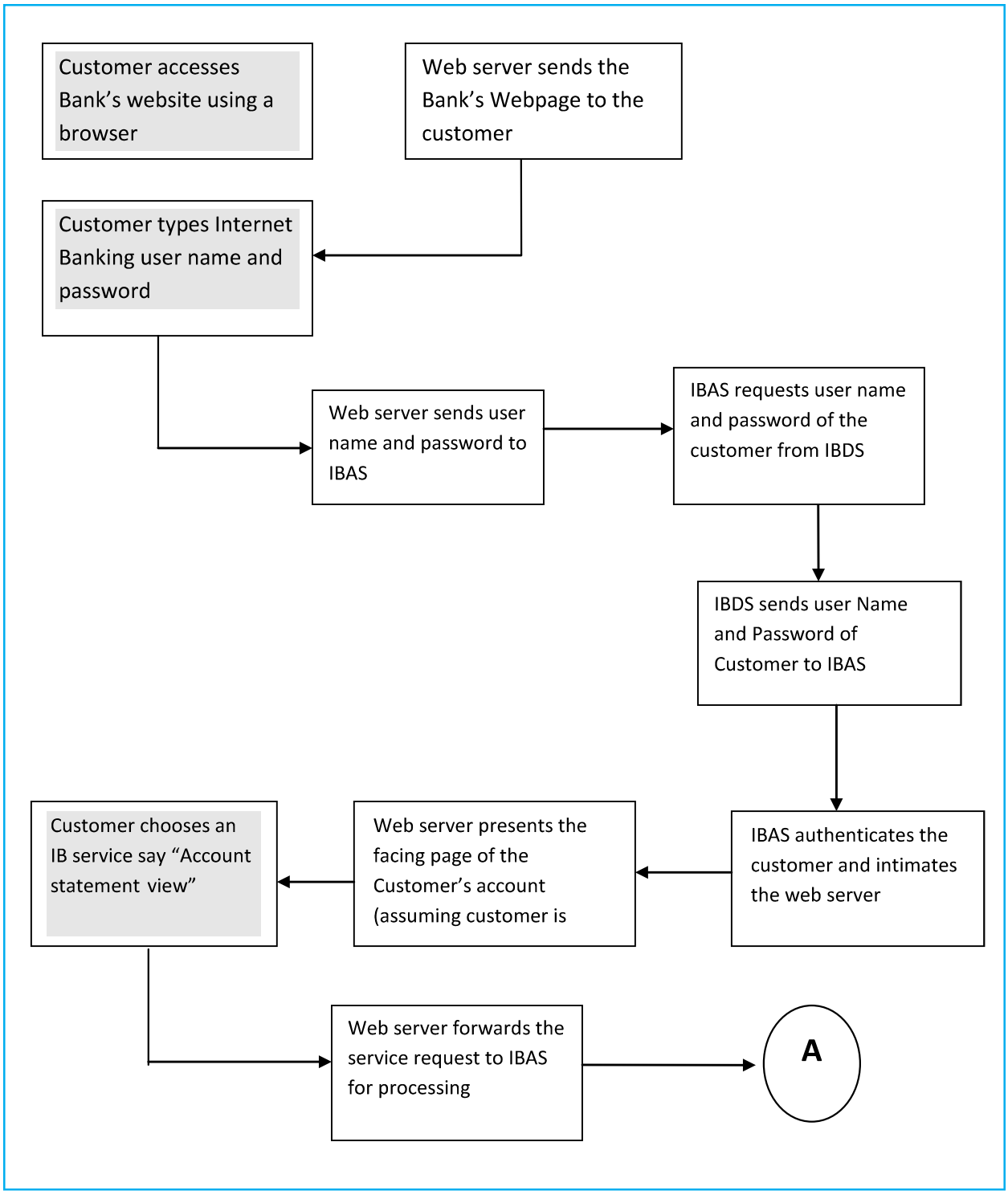


Fig 2.2.1(A): Broad Data flow diagram describing the Internet Banking Process

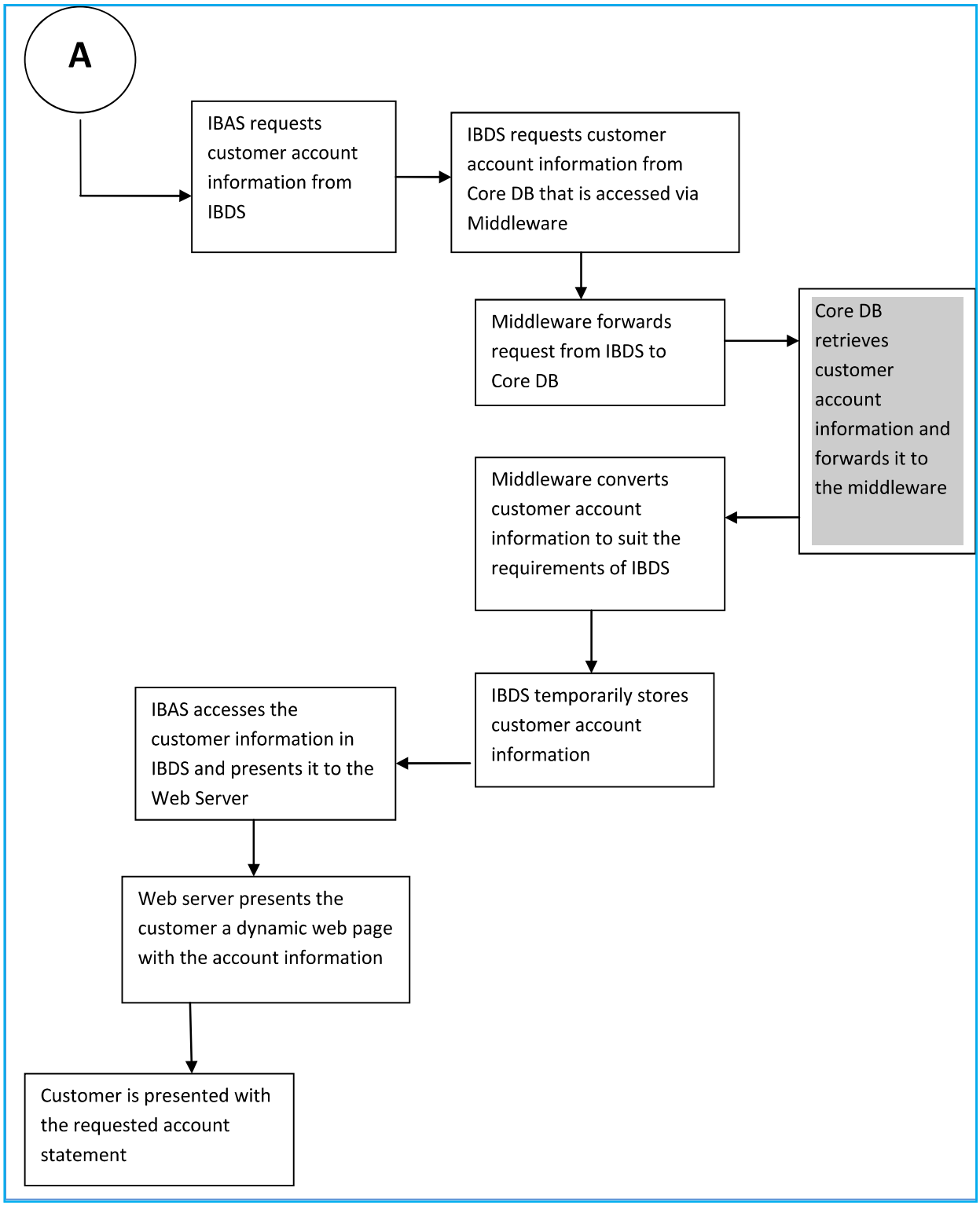


Fig 2.2.1(B): Broad Data flow diagram describing the Internet Banking Process

The customer applies to the bank for such a facility. He is provided with an User ID and Password. As is he best practice the password is expected to be changed soon after the first log on.

- Internet facility could be used only by accessing the website of the bank. For accessing the website, naturally a browser like internet explorer is used.
- The website is hosted in the web server. The web server is in the central data centre of the bank. Access to the web server is permitted only to authorised users.
- To protect the web server from unauthorised use and abuse, the traffic is necessarily to go past a firewall. The firewall is designed in such a fashion that only traffic addressed to the web server through the authorised port is permitted.
- An individual who accesses the website of bank through the browser will be able to access the web server and there will be a display of the bank's web page on the screen of the client's computer.
- The web page will also provide all information generally of interest to the public. The web page also will have a specified area wherein a mention of user ID and password will be made. Those who have been provided with the user ID and password would be expected to enter the same.
- As we are all aware, the password will not be displayed in plain text but will only be in an encrypted form.
- The web server forwards the customer details to the internet banking applications server which in turn accesses the IDBS. The server has already the data base of all the customers who have been provided with internet banking facility. For each customer, it would be having details about user ID and password.
- The information received from the web server is verified with the data of the customer held in the internet banking (IBAS).
- Should the information not tally, the message 'access denied' would appear giving the reason giving the 'user ID wrong / password wrong'. The customer realising the mistake may rectify the mistake and make another attempt. Normally three such attempts would be permitted. After three attempts, the customer will be logged out for security reasons. If more attempts are permitted, there is a possibility of a person just trying out different combination of user ID and password to break into the system.
- Based on the authentication check, the IBAS sends an acknowledgement to the web server. The web server displays the message. Once the authentication process is completed correctly, the customer is provided internet banking facility, which would include:

  (a) Password change

  (b) Balance inquiry

  (c) Fund transfer

  (d) Request for cheque book

  (e) Stop payment

  (f) Copy of statement of account and

  (g) ATM / Credit Card related queries

- The customer then chooses one of the services from the list. The service requested is directed by the web server to the IBAS for processing. The IBAS will access the internet banking data base server for further processing.
- The IBDS will retrieve the data from the central data base server. The IBDS will be able to access the central data base server only through a middleware and firewall. The middleware is expected to convert the data to suit the requirements of IBDS.
- Internet banking data base server then forwards the customer data to the IBAS which processes the transaction eg., The statement of account from the central data base server is made available to the internet banking data base server (IDBS). The IBDS then sends the data to the IBAS. The IBAS then sends the same to the web browser (internet explorer).
- The web server generates a dynamic web page for the service requested eg., the accounts statement generated by the web server and presented to the internet explorer (say) the information is provided to the web browser in an encrypted form.

The customer would be able to get the service required eg., viewing of the statement of account or a screen made available for him to request for a cheque book or instructions for 'stop payment' etc., After the services provided, the explorer may choose to log out.

Depending upon the software, the customer may be permitted to request for more than one service in one session. Some software would automatically log out the customer after one service has been completed and expect him to log in again.

It needs to be emphasised that security is a serious concern in internet banking and should be implemented with great care.

The security concerns could be:

(a) Privacy issues - customers being able to view accounts other than their own.

(b) Wrong or fraudulent fund transfers. The transfer requested by the customer may be executed wrongly i.e., instead of one account being credited or debited, a different account may be accessed.

(c) This weakness could be exploited by customers with fraudulent intentions by making unauthorised access to certain customers' accounts and transferring to their account.

PROCEDURES FOR EVALUATING CONTROLS

In any process of evaluation of controls, one needs to be aware of security concerns in an environment.

Main security concerns in Internet Banking are:

- Unauthorised access to any of the access points
- Incomplete or inappropriate procedure regarding identification of user.
- Lack of segregation of duties in the operation facilities, applications and data.
- Roles and responsibilities of system administrator not clearly defined.
- Firewall not clearly configured and monitoring procedures absent / inadequate.
- Absence of segregation of lives and test environments.
- Inadequate network security.

- Routers improperly positioned.
- Inadequacy of security of web server.
- Inadequate security of Internet Banking system.
- Inadequate security of Data Base System.
- Insufficient built in Application Controls.
- User authentication.
- Incomplete and cancelled transaction.
- Insufficient data security.
- Informal / unstructured change management procedure.

Broadly, the audit program should be on following lines

1. Security Policy

Verify whether there is a written Internet Banking Security Policy – which should include firewall policy and access policy. Overall policy guidelines should be documented and available. It should cover policy and procedures for all access points to the Internet Banking system.

The access points should include:

(a) User System.

(b) Front end application.

(c) Router, switch, firewall.

(d) Application Server.

(e) Web Server.

(f) Database Server.

(g) Network.

(h) Infrastructure of Internet Banking.

2. User Identification

Unauthorized access to other customer accounts will amount to violation of privacy rights.

Existing security mechanisms should be verified to ensure this requirement. Even weak password could lead to security lapse.

- Internet Banking Application Program should be accessible only to authorised users. In the absence of such discipline, unauthorised changes could be made to application program.
- There should be adequate logs maintained to provide monitoring facility.
- Any attempt at penetrating the network should be proactively detected by installing Intrusion detection / prevention systems.
- There should be provision to automatically log such attempts and these logs should be reviewed on a daily basis.

3. Access Control to Operation facilities

(a) There should be adequate segregation of duties. Incompatible functions should not be performed by the same individual.

(b) There should be a procedure in place to ensure that soon after an employee designs his user ID and password are revoked. His logical access should be denied.

4. Roles and Responsibilities of System Administrator

System administration is a sensitive function and should be allocated to a specific individual. He needs to have access only to perform system administration function. There should be built in control to report by means of a log if he performs any other function.

5. Firewall

It has to be ensured that internet banking services is only through a dedicated Firewall.

Periodically penetration tasks (tests to unauthorized enter the network) should be performed to ensure it is not possible

If vulnerabilities are highlighted it should be verified whether immediate corrective steps have been taken.

There should be approval from appropriate senior management before firewall, routers and other associated systems are changed or upgraded.

6. Segregation of Live and Test Environments

Like in all Computer Systems, test environment should be separate from live environment. No testing should be done in the live environment. Live environment is the environment where the live program is running. Such a program would have been thoroughly tested and moved under proper authority from test environment to live environment.

7. Network Security

There should be adequate control mechanism in place to ensure that access to both in and out of internal network are controlled.

Review whether there is any provision (usage of tools) to monitor suspicious activity.

8. Router Configuration

Routers should be properly configured to ensure that network is restricted to only necessary systems and none else.

9. Web Server Security

Web Server should run only required processes and none else. The Web Server would have its own operating system (e.g., Windows 2003) and it should be ensured that all security settings of the operating system are in order.

10. Security of Internet Banking System

A list of authorised users should be maintained and the system should not allow access to any other user.

Internet Banking system configuration should be well documented.

There should be adequate controls in place to ensure that integrity and security of transactions are not affected.

11. Data Base

Data Base should be accessible only to the Computer application in the normal course. In addition Data Base administrator has access for maintenance. There should be a log generated if any other access has been made.

Personal Identification Number (PIN) of clients which will be stored in the Data Base should be only in encrypted form.

12. Operational Controls - Built in Controls

Application should have been tested extensively so that all validity criteria are complied with before a transaction is processed.

13. Operational Controls - User Authentication

User authentication mechanism should be in the place to ensure access is restricted to authorised personnel.

14. Operational Controls - Incomplete and cancelled transactions

Procedure for incomplete processing needs to be reviewed. Special attention needs to be paid to study the possibility of a client canceling a transaction which has been entered. E.g., Fund transfer might have been entered and authorised - whether system will permit reversal - needs to be studied.

Operational Controls - Data Security

Key management procedures (for encryption) in place must be in line with best practices (Dual control)

Review whether critical data like PIN encryption keys should be stored in a physical environment e.g., in a physically secure hardware like HSM (Hardware Security Model). There should be satisfactory restart and recovery procedures in place.

Review application testing procedure for its adequacy i.e., conforming to best accepted procedures.

15. Change Management Procedure

Ensure there is a formal procedure in place for change management. Special attention needs to be paid for Emergency Procedures..

16. Library Procedures

Documenting and numbering of different version of programs, storing safely different version of programs, moving program from test environment to production environment etc. needs to be reviewed for their adequacy and conformity to standard procedures.

2.3 REAL TIME GROSS SETTLEMENT

The acronym RTGS stands for "Real Time Gross Settlement". RTGS system enables transfer of money from one bank to another on a "Real Time" and on "Gross" basis. Real time means that the transactions are settled as soon as they are processed. There is no waiting period. Gross settlement means that this transaction is settled on a one to one basis. There is no bunching with another transaction. The money transfer takes place in the books of the Central Bank of the country - Reserve Bank of India

in our country. As the money transfer takes place in the books of the RBI, the payment is final and irrevocable.

Difference between Electronic Fund Transfer System (EFT) or National Electronics Fund Transfer System (NEFT) and RTGS:

EFT and NEFT are also electronic fund transfer modes. However, they operate on a Deferred Net Settlement (DNS) basis. In DNS basis transactions are settled in batches. Transactions which take place after a particular settlement time would have to wait till the next designated settlement time.

In RTGS, transactions are processed continuously throughout the RTGS business time.

RTGS system is primarily for large value transactions. As of now, the minimum amount to be remitted through RTGS is Rs.1.00 lakh and there is no upper ceiling. In EFT and NEFT systems, there is no stipulation regarding the minimum and maximum amount. The time taken for the transaction to be effected would be within two hours. The beneficiary bank (Bank which is receiving the amount) has to credit to the beneficiary's account within two hours of receiving the fund transfer message. The remitting customer would receive an acknowledgment for the money credited to the beneficiary's account as the remitting bank receives a message from the RBI that the money has been credited to the receiving bank.

However, if the money is not credited for any reason, the receiving bank would have to return the money to the remitting bank within two hours. The remitting bank would in turn reverse the original entry - the debit entry in the customer's account.

The essential information that the remitting customer would have to provide to the bank for the remittance to be effected are:

(a) Amount to be remitted

(b) His account number

(c) Name of the beneficiary bank

(d) Name of the beneficiary customer

(e) Account number of the beneficiary customer

(f) Sender to receive information if any and

(g) IFSC Code of receiving branch (IFSC stands for Indian Financial System Code. (Explained later in the Chapter)

The beneficiary customer would be able to obtain the IFSC Code from his branch. This information is also available in the cheque leaf. The beneficiary can inform the remitting customer details regarding Code number and Bank branch.

Most of the Banks are providing RTGS service. The latest list of such branches is also available in the RBI Website.

Procedure for tracking the remittance transaction

Some banks which have the internet banking facility provide the service on line. The remitting customer would be able get confirmation from his bank either by e-mail or SMS on the Mobile phone.

Real Time Gross Settlement Process

The Banks which wish to be recognized for RTGS processing need to apply to the Reserve Bank of India to be recognized as participant banks by the Reserve Bank of India. The various steps involved in the transaction processing of RTGS are as follows:

- The customer, who wishes to remit from his account in Bank A to the recipient in Bank B, approaches Bank A.
- The transaction is entered in the client machine at the Bank A.
- The client machine is connected to a server.
- Each of the participants Bank is allotted a code number.
- This code number is called Indian Financial System Code (IFSC).
- Each of the branches of the participant bank of RTGS is allotted a unique code (RTGS Branch Code).
- A combination of these two codes referred to, act as the identification.

R.T.G.S. Technical Environment

The Diagram below explains the functional architecture of Next Generation Real Time Gross Settlement System, (NG-RTGS) as shown in Fig. 2.3.1

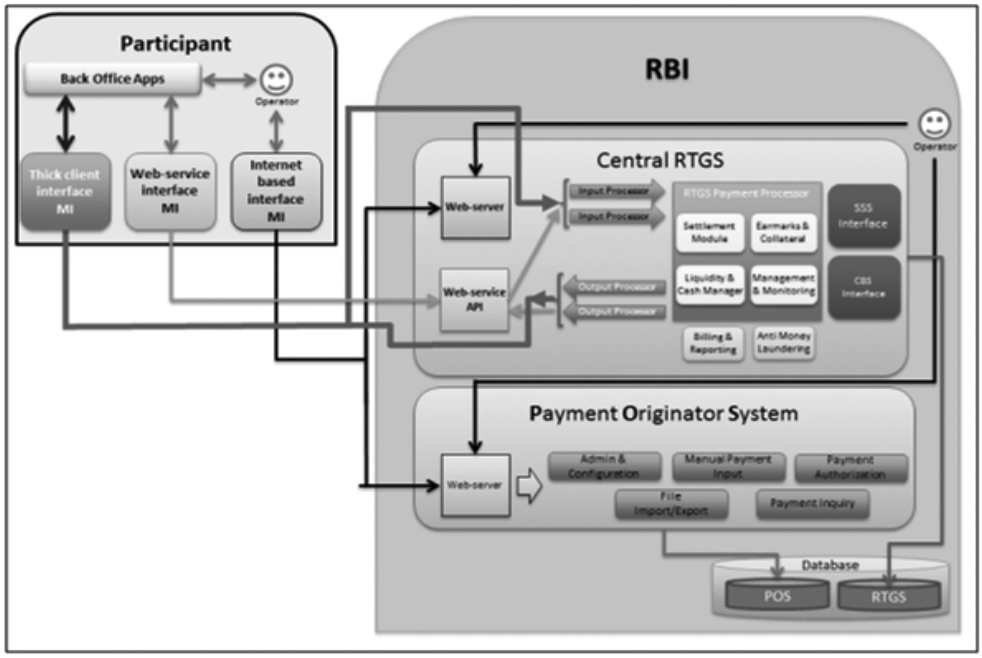


Fig.2.3.1: Functional Architecture of NG-RTGS

Features of NG-FTGS

- Interface with RBI's CBS
- STP capability with Ancillary systems

- Advanced MIS tools for report generation
- Scalability of system, including efficient and optimal threading time for transaction and capability to handle large volume of transaction
- Flexibility to add new transaction types and participant membership types
- Future value date settlement
- Balance status enquiry from central system
- Compliance to international standards including Core principles for SIPS issued by BIS
- Multi currency system
- Extended business hours
- Centralized Anti Money Laundering filtering
- Monitoring and control of payment messages

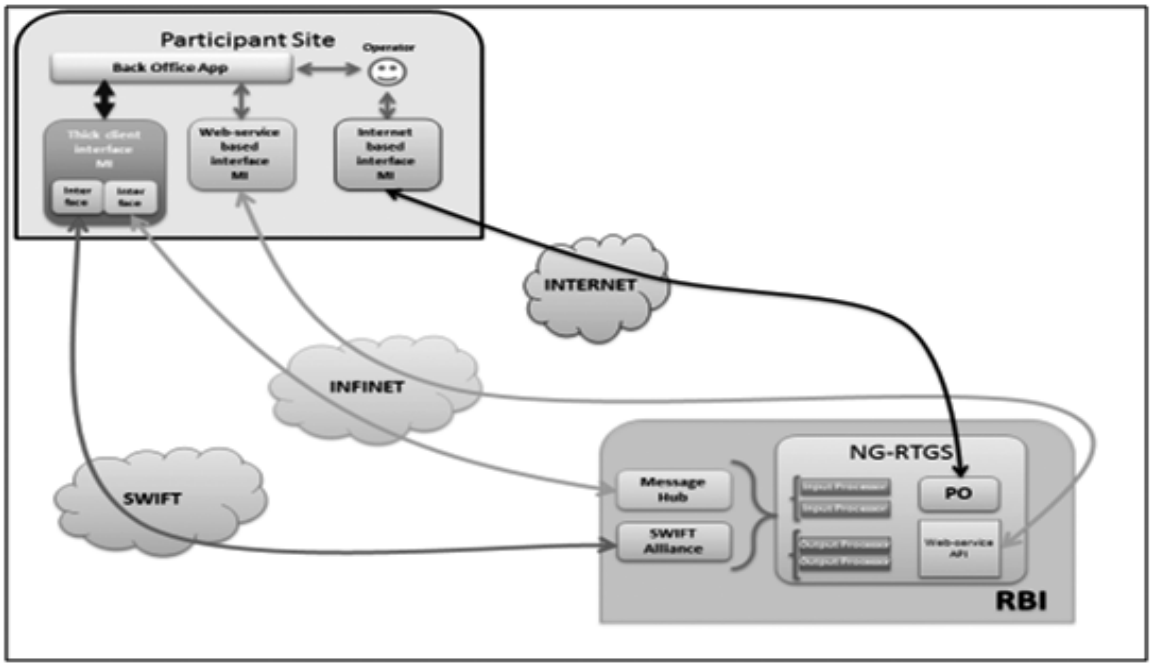


Fig 2.3.2: Communication Channels

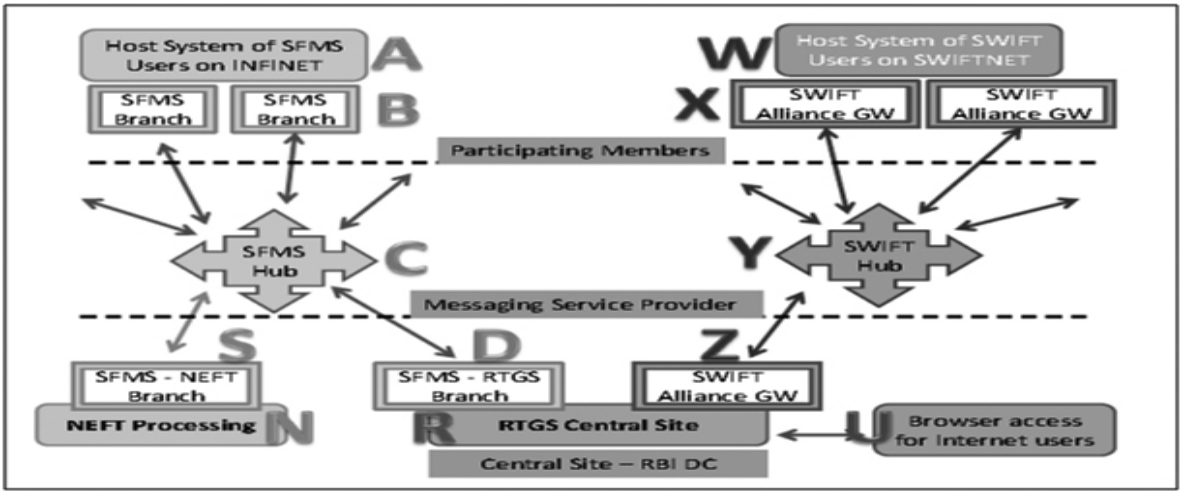


Fig 2.3.3. Design Architecture

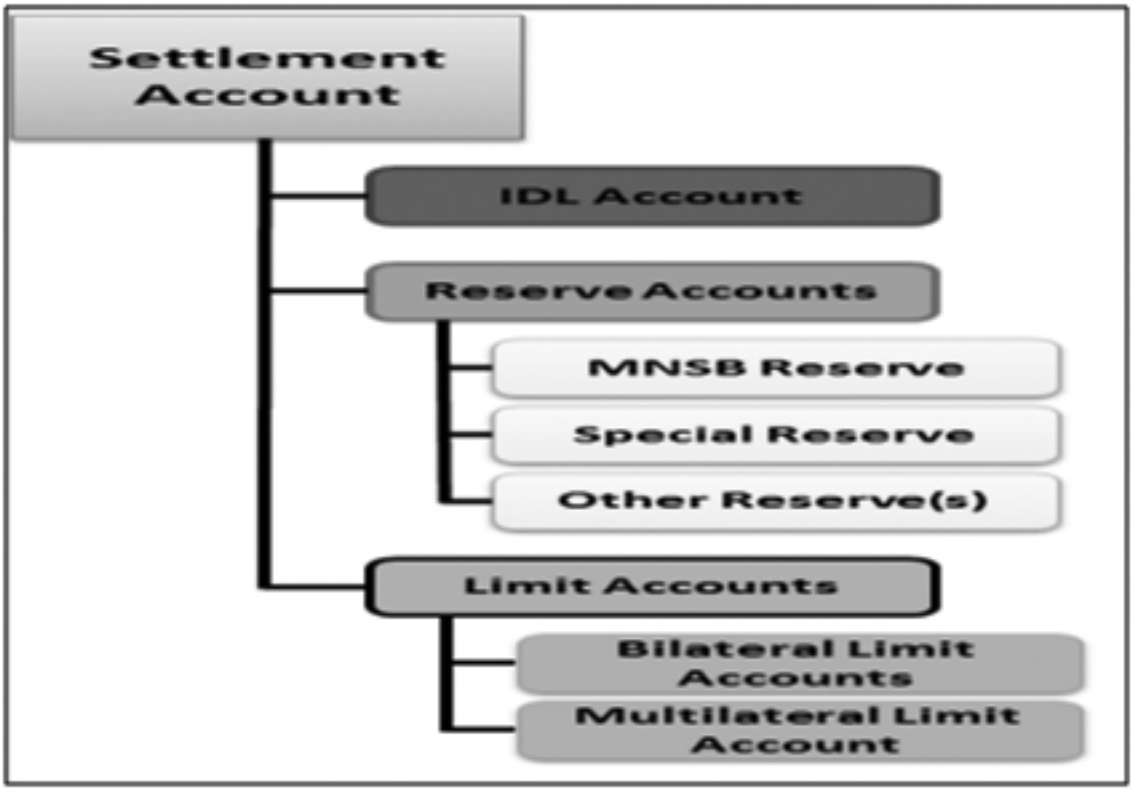


Fig 2.3.4: Settlement Account Structure

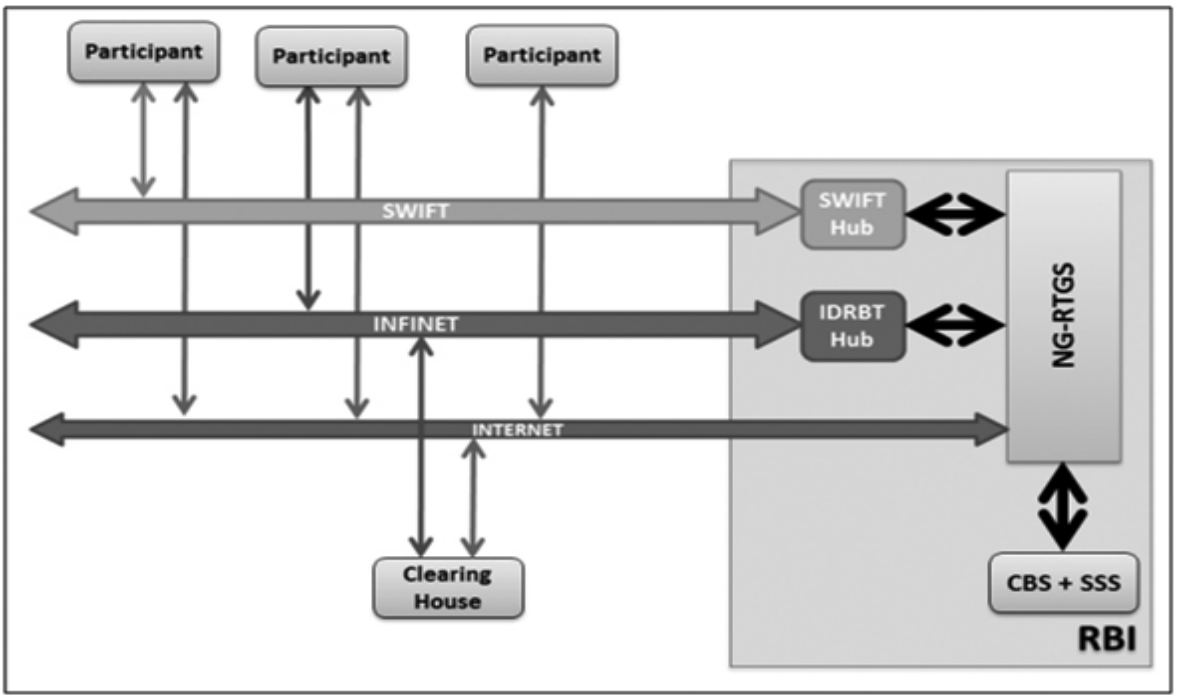


Fig 2.3.5 RTGS External Interfaces

Alerts

- Alerts are predefined, parameterized notifications generated by the NG-RTGS automatically and sent to the Participant users.
- Format:
- Visual, audible or pop-up window: delivered only to the users logged in to the Web interface of the NG-RTGS.
- Email: delivered by email to the address specified in the user's RTGS profile
- Sample alerts:
- User account was blocked due to repetitive failed login attempts
- System's timetable has been updated by the RBI
- Suspicious high amount transaction was received by NG-RTGS

MIS Reports

- Generated automatically, at predetermined moments (e.g. EOD)
- Ad-hoc, upon user request
- Format:
- XML (ISO camt.053), PDF, Excel (CSV).
- Availability:
- Online, as file download from the central NG-RTGS

- As email attachments for EOD statements
- Content:
- Analytic reports of the RTGS activity: summary of the transactions, net position, chargingreports etc.

Benefits of new messaging System

- The standard supports end-to-end inter-operability.
- ISO 20022 is more powerful to represent complex data structures (because of its modeling approach and XML data representation.
- It offers synergies with other payment instruments and markets allowing for convergence into a single platform.
- It reduces the impact of proprietary technology.
- It is independent of transport mechanism
- It allows easier adoptability to payment system participants to connect to their varied functional systems & channels with low investment.
- Availability of and access to growing pool of technical resources and expertise on technologies used in the standard.
- ISO 20022 enables use of inexpensive and widely available tools for basic data manipulation & simplifies integration with XML enabled applications and processes.
- Majority of format & business validations can be implanted inside ISO 20022 thus minimizing application level coding requirements.
- XML approach allows incremental expansion for scope as and when new business case arrives with no changes to the processing system to accommodate or validate the message
- It helps improve straight through processing.
- It reduces the impact of maintenance.
- Standardized validation processes.
- Faster and more flexible development if messages needed to be extended.
- Standardized status & error codes.
- End-to-end customer references (with more characters than are used today).
- Fewer processing errors, due to consistent formatting standards.

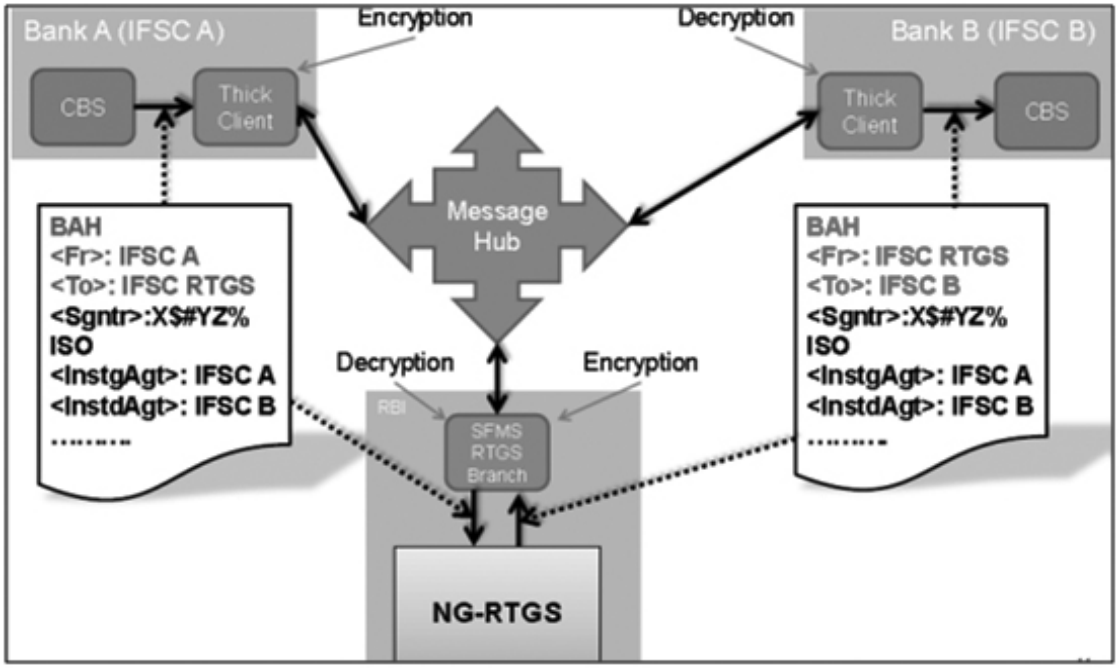


Fig.2.3.6: Message transformation in NG-RTGS

SMS securities settlement scheme

In the initial days of RTGS, transactions were manually keyed into the member institutions account system and into the RTGS system. These two independent manual operations often led to data inaccuracies. But today many member institutions have implemented Straight Through Processing (STP) modules. STP implies that the member institutions software system and RTGS software talk to each other through defined interfaces. As a result it is sufficient if data is entered in one system only and it automatically flows into the other. Thus an outward remittance transaction is entered into the member institution's system (say, a Bank's Core Banking System) and it is automatically processed and posted into the RTGS PI. Similarly an incoming remittance transaction automatically flows from the RTGS PI to the member institutions accounting system.

A special feature of STP is that Uniform Transaction Reference (UTR) number for any outbound RTGS transaction is generated by the STP system. However, such a message has to be necessarily routed through the RTGS Member's PI to RBI's IFTP system.

Obviously STP system requires that the member institutions internal processes and back office functions are robust and reliable. Incidentally some of the big banks now allow their customers to initiate an RTGS remittance transaction through the bank's Internet Banking facility also.

Important Security Features of RTGS

Unique Transaction Reference (UTR) Number:

Every message, sent by the member bank to the RTGS system is allotted a Unique Transaction Reference (UTR) and this number is embedded in the RTGS message itself. This UTR is used by the parties to identify the transaction among them for any enquiry / investigation / complaint. A message without a UTR will be rejected by all systems forming part of the RTGS.

Also every message released by the member bank to the RTGS system will be assigned a Sequence Number (SN). The Sequence Number (SN) is continuously incremented with every message. Therefore, any message, received at the RTGS system with a SN, which is not the next expected SN from the concerned member bank, will be rejected by the RTGS System.

Handling Duplicate Messages:

If the RTGS system receives a duplicate copy of an earlier message (i.e., two messages with the same UTR and contents), then it will be treated as a duplicate. It will not be processed by the RTGS System. In case a response to the earlier message had already been sent, then the same response will be sent again. Also the response will be marked as a potential duplicate emanation.

On the other hand, if the contents of the duplicate message (i.e. message with the UTR as an earlier one) are difference from those of the earlier message, then the RTGS system will consider the situation as a breach of security and will disconnect the PI associated with the duplicate message. However, such situations are rare.

2.4 CASH MANAGEMENT SYSTEM (CMS)

Cash Management System (CMS) is a new product developed by banks. The objective of the product is to meet the needs of the customers who have operations all over the country. Such organizations would naturally have collection and payments in various locations.

In the normal course, cheques would be collected in one single location and then deposited in the main branch. This causes cash flow problems as there is uncertainty regarding the dates when the cheques would be realised. In view of this uncertainty both scenarios of excess cash and deficit cash were arising. As in receipts by way of cheques a similar situation arises when a high volume of disbursement has to be made e.g.,

(a) Salaries for the different branches

(b) Dividend payments.

To get over these problems of cash management and to make the process of cash management effective, banks have introduced this new product - CMS. The broad features of CMS are as follows:

- Multiple collection centres have been authorised to receive the cheques / drafts of the customers.
- It is not necessary to open a separate account in each of these centres.
- At the client's main account which is maintained at the pooling centre credit is offered on the same day for all the cheques / drafts deposited and cleared at the branches.
- The product also provides Management Information System to customers providing details location wise and also party wise.
- If necessary, information can even be provided by e-mail.

Evaluation of Controls of CMS:

Parameter settings (Master Settings): There needs to be adequate controls over parameter settings, authorization as also modification of such settings. E.g., Parameters would include:

(a) Clearing cycle

(b) Credit limit

(c) Charges (various slabs)

(d) Interest (")

Processing Charges: When the bank offers CMS product to the customer, naturally there are associated charges for the same which would include:

(a) DD / Pay Order issue charges

(b) Courier Charges

(c) Cheque return charges

(d) Interest charges for credit offered.

There needs to be a process logic for computing the various charges. Any defect in the logic would lead to income leakage. While evaluating the controls, it is necessary to verify the correctness of the parameters and also test the program logic. It is important to verify the authorization process for creating and modifying parameters.

In certain circumstances the customer may be offered a credit limit which exceeds the sanctioned limit. This can be done only under proper authorization. Aspects of this nature need to be verified at the time of performing the audit.

End of Day Processing

The various amounts collected and different amounts disbursed are all pooled in a designated account. There needs to be a control to ensure the accuracy of such pooling.

The CBS product is interfaced with the core banking solution. The charges and other items need to find a place in the general ledger. Mapping of entries need to be verified. It should also be verified whether there is a built in control to prepare an exception report in case of apparently wrong entries e.g., collection charges being credited. Normally the CMS product provides various audit trails which include listing of parameter settings, transaction authorization and waiver charges. While evaluating the trails and performing the audit, the adequacy of audit trials need to be verified.

CHAPTER 3

SYSTEMS AUDIT OF CBS AND ITS INTERFACES

LEARNING OBJECTIVES

- Introduction to ISA
- Evaluation of security and Controls in CBS
- CBS control and Audit of branches
- Using reporting / SQL feature for analysis, reviewing controls at different layers with case study.

3.1 INTRODUCTION TO INFORMATION SYSTEMS AUDIT

Systems auditing is an important aspect in the present context of extensive computerisation. The control objectives and audit objectives always remain the same. However, audit methodology in a computerised environment is distinctly different from that in a manual environment.

In 1967, in the United States, a significant event took place in history of systems audit. It is commonly and popularly referred to as the "Equity Funding Case". The Managers and Directors of Equity Funding Corporation of America, with the idea of increasing the share value of their company profits were falsified by creating bogus insurance policies. Apart from that, other methods were also used. The auditor for the parent company was not the auditor of the insurance company. This was done with the main idea of confusing and confounding the audit process so that over dues could not be detected.

These matters were further complicated by the external auditors confirming the existence of the insurance policies (the faked ones)! The confirmation was obtained on the telephone. It was reported that the calls went through the equity fund switch board to the employees who were colluding with the managers and they confirmed the existence of the policies.

In 1973, after nearly six years, the fraud was exposed, that too by a disgruntled employee who alerted the authorities. Thereafter the Stock Exchange suspended trading of Equity Fund shares. A leading audit firm with partners who had necessary knowledge and experience to perform audit in a computerised environment was appointed. It was discovered that US $2.00 billion worth of bogus insurance policies were there. Thereafter all the things that happened is history.

The fact that came to light was that the original external auditors missed out many clues that there was an apparent fraud. The management to proliferate the bogus insurance policies had used the computers to take advantage of their speed. The computer files contained details of the policies, a mere reading of which would have highlighted the fraud.

The importance of performing systems audit was very much appreciated as the cause for the non detection of the fraud was more because there was lack of knowledge on the part of the auditors. Though some auditors colluded in the equity funding case provocated a well-known authority on the subject of systems audit to comment that the equity funding case contributed a great deal to systems audit! He further said that recognition and development of the systems audit than any other single event. The case had however certain other positive effects too. The management which previously did not want the auditors to be "snooping around" the computer department changed its attitude and welcomed the auditors and their report.

The management sought an independent assurance as to whether the information systems on which they rely is dependable in terms of controls, were built into the system or outside.

Confidentiality, Integrity and Availability (CIA) are the components of information security. Systems Audit, which verifies the controls in a computerised environment evaluates the controls and provides assurance regarding adequacy.

In a banking environment, where all of manual maintenance of accounts have been shifted to computers, the importance of performing systems audit can never be over emphasised.

Many controls for information systems and important ones at that are built into computers. Hence as verification of internal controls are of utmost importance, systems audit as distinct from manual audit assumes importance.

With the Core Banking Solution being implemented, the computer technology has become more advanced and all of the operations at all of the branches are all networked to the Central Office. The hardware and the communication are distributed and the software is centralised. Audit objectives of performing audit of banks have not undergone any change. However, audit methodology has undergone a 'sea change'. Reserve Bank of India has in these circumstances issued many circulars which are available in the RBI website - www.rbi.org.

The Institute of Chartered Accountants has issued guidelines for performing audit in an information technology environment. As of now, many of them are as guidelines and hence though not mandatory, members are expected to comply with the requirements. One such important guideline came in the name of Gopalakrishnan committee report which is taken as a mandatory guidelines by RBI.

In certain cases, the RBI has as a prerequisite instructed that systems audit should be performed before implementation of certain products e.g., internet banking. The bank would not be permitted to commence internet banking operations unless the requisite security and controls have been certified by a competent systems auditor.

3.2 SECURITY AND CONTROLS IN CBS

In any information technology environment, there are certain controls and standards to be adhered to. When specific products like internet banking, ATM. RTGS/ NEFT, and CMS are introduced, there are certain additional controls specific to those systems which have been discussed in the respective chapters. In the following pages, we would be discussing the security and controls which need to be in place. Given below are the broad specifications of controls. Under each head there are other specific controls. The main heads would be

(a) Management Controls

(b) Organizational Controls

(c) Operational Controls and

(d) Application Controls.

(Infrastructure controls already covered in previous chapter)

Management Controls

Management controls would include (a) formulating a security policy, (b) developing a business continuity planning and (c) laying down procedures for systems development.

Security Policy

Security Policy is a document approved at the Board level. Reserve Bank of India mandates that every bank should have a security policy. The contents of the policy at the minimum should cover the following:

1. Formation of Security Committee/ Steering Committee
2. Asset Management
3. Human Resources Management
4. Physical and Environmental security
5. Communication and operative management
6. Access Control
7. Systems development and Change Management Procedure

Business Continuity Planning

There should be a comprehensive document in place taking into consideration critical operations of the bank. Reserve Bank of India mandates on every bank having a Business Continuity Plan in place. From the accounting point of view, one needs to look at it from the "going concern concept". The existence of a Business Continuity Plan, evidence of testing and evidence of updating are essential. The various likely scenarios of business interruptions should be envisaged and a plan to meet such situations and keep the business going should be documented. There should be evidence of awareness being created among the employees.

Systems Development and Change Management

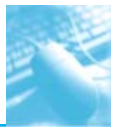
Best practices for development of systems and change management should be documented. Constant monitoring of its being complied with should be in place. The procedures would include program development, program testing, and movement to library, movement from library to production, roles and responsibilities of Computer Team members, highlighting incompatible functions.

Organizational Controls

Organizational Controls would include the organization structure of the IT Department, IT Strategies roles and responsibility including incompatible functions would include.

Operational Controls

This would include physical access, logical access, environmental controls, evaluation controls in operation systems and evaluation controls of network.



Application Controls

The controls would broadly come under the following heads:

- Input
- Output
- Process

Input

The input controls would ensure that the data entered is complete and correct. To ensure the same the following built in checks would be in the application software.

- Data validation
- Reasonableness check
- Format check (Mandatory files)
- Range check

Process

Controls ensure that the software comprehensively covers the business process in the different modules. Process control would also include the existence of built in controls in the system to ensure proper processing of input data so as to provide the required output.

Core Banking Solution

The various application modules which would normally form part of the total Core Banking Solution would be

(a) Customer ID generation (create a customer with a specific No.

(b) Accounts Management. (To ensure that the account opening process is in line with the bank's laid down procedures. This module will deal with creating savings account, current account, cash credit account, overdraft etc.,

(c) Savings Bank and Current Accounts

(d) Fixed Deposits, Recurring Deposits and other Term Deposits.

(e) Cash Operations Module

(f) Clearing Module - which would include inward clearing as also outward clearing?

(g) Bank Guarantee: This module would cover bank guarantees issued by the bank on behalf of the customers in favour of third party's guaranteeing to fulfill the terms of the guarantee. Guarantees may be in the nature of

  (i) Performance guarantee or

  (ii) Deferred Payment guarantee.

(h) Bills: Bills involve trade transactions and would include

  (i) Clean supply of bills

  (ii) Payment Usance Bills

(iii) Outward Bills (Cheques)

(iv) Inward bills

(i) Letter of Credit: Letter of Credit refers to an arrangement wherein the issuing bank acts on the request and instructions of a customer.

(j) Remittances: This process involves remittances of money by way of DDs or Money Transfers etc.

(k) Advances: The banks collect demand deposits and term deposits. Out of the funds collected they maintain Statutory Liquidity Ratio (SLR) and Cash Reserve Ratio (CRR) as per the RBI's requirements. Out of the balance funds available they lend to priority and non priority sectors.

The functionality of each of the modules has to be comprehensive.

l. Master Maintenance - the core banking solution would need to have master data

(i) Parameter setting for account type and structure settings keeping in view the General Ledger

(ii) Parameter settings for interest rates applicable. These interest rates would vary for different parties e.g., staff, senior citizens etc.

(iii) Rates would vary also for the tenor deposits eg. 1 year, 2 years etc.

The parameters should be entered into the system with due care. The updation of the parameters is more important if not more than the original creation. Other examples of critical parameters used by CBS applications would include list of holidays, authorization rights for exceptional transactions, list of deposits, penalty payable in case of default in RD etc., defining various warning, exceptions, error codes, work class of various user, type of user etc.

Operational Parameters

Given type wise operational parameters - TDS, Anywhere banking parameters.

Charges Parameters

Standing instructions charge, Stop Payment instruction charge, cheque book issues, account closing charges.

User Related Password Change Parameters: validity, password history, length, structure etc.

Interest related parameters

Term Deposits interest rates, Interest calculation for advances, interest calculated for staff, loan interest calculation for senior citizens – frequency, start date, end date, fised-flexible, simple-compound etc.

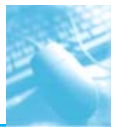
Authorization Parameters

Authorization of users varies for exceptional transactions.

Log Maintenance

Logs are record of activities that have taken place in the system irrespective of the modules. The contents of the log would include:

- The activity



- The user (system)
- Date and Time

These logs need to be preserved carefully as they are the conclusive and relevant evidence to prove that a transaction occurred. Naturally the logs should not be capable of being modified. The logs should be accessible only by the authorised person and by none other.

The points discussed above provide an over view of controls that need to be in place in a Core Banking Solution.

3.3 AUDIT OF CORE BANKING SOLUTION

Audit is the process of evaluating the adequacy of controls and also ensuring relevant application modules deal comprehensively with business process. The various aspects to be verified while performing the audit in the Core Banking Solution environment would be:

(a) Review of Security Policy

(b) Review of Business Continuity Planning & BCP policy

(c) Review of Systems Development and Change Management Procedures & process

(d) Network vulnerability Assessment of Effectiveness of Intrusion Detection Systems.

(e) Evaluation of controls in operating systems.

(f) Control in databases

When any of the services like software development, database management, network management are outsourced, review of the service level agreement to ensure that confidentiality integrity and availability are taken care of is extremely important. Service level agreements should provide for a systems auditability clause. So that Banks will have the right to have systems audit conducted of the third party services.

(g) Testing of application modules of the Core Banking Solution.

(h) Review of Systems logs.

(i) Audit of Internet Banking, Audit of ATM and RTGS/ NEFT also need to be done and these have been considered separately under their respective heads.

That means IS Audit of outsourcing activities should form part of IS Audit of Core Banking.

A. Review of Security Policy

Reserve Bank of India has mandated that every bank should have a security policy which is approved by the management. The document should be constantly updated. There should be awareness of the contents of the security policy amongst the employees as applicable to different operations. The security policy applies to the entire organization and to all of its employees, customers and also to third parties to whom services have been outsourced.

The broad contents of the security policy should be

1. Formulation of a security committee to manage information security within the organization.

2. Asset Management: The policy would deal with the procedure for maintaining proper protection of organizational assets. The assets need to be classified according to their sensitivity and criticality to the organization.

3. Human Resources: This would deal with procedures to be followed in connection with the employees, contractors and third party users. There should be procedures to be followed under the following circumstances.

   (i) Prior to employment

   (ii) During employment and

   (iii) On termination or change of employment.

   Before employing, background verification should be done. During employment, there should be absolute compliance of the requirements of the security policy. A formal disciplinary procedure for violation of the security requirements should be in place.

   On termination all access rights to information processing facilities should be removed immediately

4. Physical Environment: Procedures should be in place to ensure unauthorized access, damage or interference is prevented.

5. Communications and Operations Management: Operating procedures should be documented and proper segregation of duties should be implemented, where appropriate, to reduce risk or intentional systems misuse. This would also apply to outsourced third parties.

   The other aspects would include network security management policy, e-mail policy, firewall security policy, internet policy etc., access control policy, cyber security policy etc.

6. Media Handling: It is important that media should be disposed off securely and safely when no longer required. This would prevent leakage of data specially the sensitive data.

7. Access Control: There should be an Access Control Policy to control access to information which needs to be reviewed based on business and security requirements. There should be a formal user registration and deregistration procedure. Allocation of password should be controlled through a formal management process. There should be a regular review of user access rights at frequent intervals.

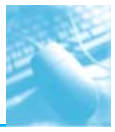
   Users also have their own responsibility and should follow the security practices, e.g., selecting passwords, having a clear desk etc.

8. Network Access Policy: Access rights should be purely on a need to know basis. Groups of information service users and information systems should be segregated on networks.

9. Operating System Access Control: Access to operating system should be controlled by a secure log on procedure. There should be proper monitoring procedures in place.

10. System Acquisition Development and Maintenance: Best practices should be in place for program development, testing, modification, library maintenance and also back up procedures for programs and data.

11. Information Security Incident Management: In spite of best intentions and documentations, there could be a security lapse. Any such incident notices would be required to be reported to the appropriate management channels.



B. Business Continuity Planning

A well managed process should have been developed and maintained for business continuity throughout the organization. Thus information security is needed for the organization's business continuity. Business Continuity Planning should be tested and updated regularly.

(a) **Compliance with local requirements:** There should be appropriate procedures in place to ensure proper compliance and legislative, regulatory and contractual requirements.

(b) **Review of Business Continuity Planning:** The Business Continuity Planning is a process by which the bank ensures the maintenance and recovery of operations. The objectives of Business Continuity Planning would include minimizing financial losses, continue to serve customers without interruption, and keep up the image of the bank. The Business Continuity Planning is distinct from Disaster Recovery Planning (DRP). The Disaster Recovery Planning has the objective to plan to recover from the impact of disaster, to bring back support service and to restore normalcy. The Business Continuity Planning should take into consideration critical business functions and priorities them. The plan should cover the following important & critical processes:

- Branch Operations
- Administrative Operations
- Internet Banking
- ATM Operations
- RTGS/ NEFT
- All other alternate delivery channels

The various disaster scenarios need to be considered and a few examples are given below:

- There is no access to the Computer Services Department building and also to the Data Centre.
- There is access to the Computer Systems Department building; but Data Centre cannot be accessed.
- The main server at the data centre would have gone down though access to systems department is available.
- Computer systems department and data centre site are available but connection to all branches and Head Office is unavailable.

The various likely scenarios need to be envisaged and a plan has to be in place so that the bank's business operations are carried on without interruption.

So, while auditing, we need to verify whether there is a Business Continuity Plan and whether it has been tested and whether it is constantly updated.

C. Review of Systems Development and Change Management Procedures: Core Banking Solution software will consist of many modules. System Development refers to the process of developing software which would produce the required output from the input provided of course, using the necessary hardware and communication systems. The systems whether supplied by outsiders or

developed in house should meet the deliverables, accepted and approved by the management. The objectives of audit would include reviewing the following:

(a) Whether the systems are implemented with adequate internal controls.

(b) Whether the business functionality is comprehensive.

In a banking scenario the management may requisition the services of the audit for implementation or while in the process of being implemented. Irrespective of when the audit is going to be done, there needs to be a procedure which is strictly adhered to as far as development of systems. There should be a formal request from an authorised person. The programs after they are developed should be tested in a test environment. The programs would be tested for functionality and adequacy for internal controls. When programs are tested certain inadequacies and deficiencies could be discovered. It would go back to the Programming Team for correction. Again it would be tested. This is an iterative process. It is important that whenever a program is changed to set right a particular situation, the entire program should be tested. This would ensure that the changed program continues to perform in the same manner in all other aspects before the change was implemented.

Process of moving a tested program from the Testing Environment to the Production Environment.

The Development Department and the Production Department should be separate and isolated. Under no circumstances should any members of the development team have access to the production environment. These aspects have been discussed in detail while discussing the organization structure of a computer department and incompatible functions.

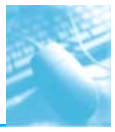
A completely tested program from the development department should be moved to the library and the librarian should move the same to the production environment with full documentation being maintained.

Change Management:

However, well developed software, it could require to be changed. This could arise either due to additional business process requirements or technology changes as also additional bugs being discovered.

There should be a formal and well documented procedure in place for changes effected. There should be a register maintained to keep a tag on different versions in the program. These registers could also be maintained on the computer.

(d) Network Security: In a core banking solution, as discussed in the earlier chapters, there is a complicated network system. All the servers (Application Server, Data Base Server, Antivirus Server, Web Server, Internet Server etc.,) are all at the data center in a central location. The branches are situated all over the country. ATM kiosks, e-lobby are situated in different places and customers are accessing the facilities from different places. Customers are provided internet banking. In view of all these facilities, we can imagine the complicated network which has to be in place. In view of this network security assumes great importance. Performing the vulnerability assessment of a network, it requires technical knowledge. However, it is necessary that network vulnerability assessment is performed periodically by competent people and a report should be available. Weaknesses in the communication systems which would have been highlighted need to be plugged. Vulnerability assessment is a continuous process. 'Patches' (solution for dealing with vulnerabilities discovered) are made available on the net. The network administrator is to constantly be applying the patches. If the patches are not updated and the weak points highlighted by the vulnerability assessment is



not attended to immediately the bank's network is open to exploitation. It can easily be hacked. To prevent such security lapses, it is imminent that vulnerability assessment is performed by competent people. There are certain tools available which properly trained people can use.

The systems auditor must verify whether constant network vulnerability assessments have been performed by the competent people. Similarly, it is also important to ensure that intrusion detection and intrusion prevention is taken care of. There are tools again which could be used by competent people, who would evaluate the strength of the network and detect if there are any weak points, which could be exploited by an intruder.

(e) Evaluation of Controls in Operating Systems: Operating System is a set of computer programs that manage the hardware and software resources of a computer. Operating systems contain the whole list of policies and the systems administrator administers the policies. It is the responsibility of the system administrator to ensure that all patches applicable to the particular operating system are applied. The systems administrator should also ensure that unnecessary services and facilities are disabled. Applying of patches is an ongoing process. An Administrator Guide is available with every operating system and it provides all important information including implications of security settings. Proper testing is required before applying any patches.

(f) Testing Application Systems: This process consists of independently ensuring that computer systems (hardware, software and communication systems) produce the required output from the given input. Each of the modules needs to be tested. The auditor needs to be knowledgeable of the business process of each of the modules e.g., Savings Bank Account, Current Account, Fixed Deposits, Loans, Bills etc.,

Procedure for testing:

The Bank would be required to provide separate systems complete with copy of the Core Banking Solution software, data base, master files etc.,

The auditor should request the bank to create at least two user IDs and passwords. The software has to be the exact replica of the one running in the live environment i.e., the version number should be the same.

The auditor will verify all the application modules one by one to verify the completeness of the functionality, built in controls in the system and controls if any outside the system.

Broad guidelines for testing one of the modules viz, Fixed Deposits are provided below:

When the system is switched on, it will ask for the user ID and password. The auditor should give the user ID and password provided by the Bank. He should take necessary steps to change the password, as otherwise the accountability for the usage of the computer would be lost. There will be a screen which would give the option for choosing the module. The FD module could be chosen. A study of the flow of the process for the FD system and the various screens need to be initially studied to get an over view.

The FD system cannot be tested straight away as a customer would need to be created. KYC (Know Your Customer) norms required by the Reserve Bank of India need to be complied with.

Now the process to be tested is FD system. Choose one customer and create a cheque deposit for the deposit account. Naturally unless the customer is got adequate funds the cheque cannot be honoured. So the program has to verify the same presuming that there are enough funds. Data for the cheque is keyed in the relevant screen.

The auditor is always testing to verify whether system will function properly under specific conditions. In principle, a post dated cheque should not be accepted. For testing purposes the auditor can try to enter a cheque with a date which is beyond the system date. Having entered the data on the screen, the user can now press "accept". If the programme is working properly, the computer would pop up a message "cheque date beyond system date" or similar message to convey that it is a post dated cheque. Whatever be the attempts made, the cheque should not be accepted by the system. Similarly a cheque not belonging to the customer or a cheque belonging to a customer but the customer is having no balance could be one of the many testing conditions. In case an error message is flashed, corrective action needs to be taken and the data is properly entered.

However, the system should not accept it unless another individual authorises the same. The entry should wait for authorization. The authorization should be capable of being done only with another user ID and password. This concept is called "maker-checker concept". This is very essential as this ensures there is dual control. To test the "maker-checker concept", the auditor can try to authorise a transaction using his user ID and password. The system, if correctly functioning, should not accept the operation. It should flash a message similar to "illegal". Similarly after an authorization has been completed properly, none of the entries should be amenable to modification. Hence the auditor can try to change any of the fields like maturity date, amount etc., That should not be possible.

Presuming there are no errors in logic after passing through certain sequential menus, the FD would be created in the system depending upon the tenure (one year, two years etc.,). The interest rate will be picked up from the master data. One of the earlier screens may require information regarding the customer type. When it expects them, we should provide information regarding the customer like 'senior citizen', 'staff member' etc.

Based upon the customer type and time period of FD, the programme (the CBS software) will look up the parameterised table and choose the correct rate.

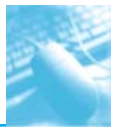
If parameterization of master data is not correctly done (and also not tested properly), naturally an incorrect rate would be picked up. Under normal circumstances, these basic components of the program would have been tested before releasing the same. However, the auditor who tests these aspects as while changing the rates, errors are likely to crop up.

The auditor could test it for other aspects like pre closing of FD, for issuing of duplicate receipt etc., while testing for the pre closing, the auditor would verify whether the logic is working properly like applying the appropriate penalty rate and making proper adjustments against the amount payable to the customer. In the case the application for issue of duplicate FD receipt, the system should verify whether the original FD is in existence and also before issuing a duplicate FD receipt that fact should be noted in the system by "flagging -the FD record in the computer system". If such a procedure is not in place, possibilities of amounts being repaid both on the original as well as on the duplicate cannot be ruled out. This may be discovered much later!

This extensive and exhaustive testing of the program depends entirely on the in-depth knowledge of the auditor and his capability to test the system in different conditions.

All of the application modules in core banking solution would need to be tested similarly, taking into consideration the respective business process and accepted built in controls.

Testing of internet banking, ATM, RTGS as mentioned earlier are not considered here as the same have been dealt with separately.



(g) Review of Systems Logs: Logs as already mentioned are reports generated by the system automatically. However, it needs to be mentioned that they generate automatically once it is programmed to do so. Auditors should review the systems logs. The systems logs could be classified as:

(a) Operating System Logs

(b) Application Logs and

(c) Data Base Logs

Above are exclusive of logs generated by network devises.

Operating System Logs:

Depending upon the operating systems (Windows-2000, Windows 2003, Unix etc.) logs are generated containing authentic information related to security. The concerned administration manual of the operating system would provide enough guidance to evaluate security concerns, if any.

Application Logs:

Application logs are logs generated by the application programs. While developing the programs, decisions are taken regarding the aspects to be reviewed and logs to be prepared.

In banks, logs would be generated for loan authorisation, limit creation, preclosure of deposits & all such activities etc.,

A review of these logs would provide information to the auditor for security evaluation. The system could also be programmed to provide to generate exception reports. An auditor should collect details about exception reports which have been generated. The exception reports could include:

(a) Account opened and closed during the month and

(b) Loan Arrears and

(c) Temporary Over Drafts granted etc.,

Date Base Logs:

These logs are available only for the computer systems department and could be viewed only by an authorised user like data base administrator. There could be other significant data base logs to review changes at the data base level but not through the application. This is a matter of serious data concern,

The log management is essential to ensure that computer security records are stored in sufficient detail for appropriate period of time.