ABM-503

UNIT-V

Ancillary Services and E- Banking: Remittances, DD, MT, TT, Traveler's cheques, bank orders, credit card, debit/smart cards, safe deposit vaults, Electronic fund transfer, Internet banking, mobile banking, ATM banking, E – Cheque, authentication, Cyber Evidence, Banking Ombudsman

Over the years, especially in the later part of the 20th century, the Indian Banking Sector has undergone fast growth and with the advent of technological changes, Indian banks are adopting to the new environment. The two successive Committees on Computerization (Rangarajan Committees) were responsible for bank computerization in India. Over the years led by the initiatives of the Reserve Bank of India, banks in India have witnessed lot of changes into their banking operations duly supported by IT and communication revolution. Some important areas where the IT plays important roles are:

Funds Transfer mechanism: ECS, EFT, RTGS, NEFT

Clearing House operations: MICR, CTS

Innovative on line e- banking services: Tele banking, Mobile banking, SMS banking, Credit/ Debit Cards, ATMs, Internet banking, Core Banking Solutions, etc.

IT and Communication Systems – Important features

The integration of computers and communication techniques has opened opportunities for banks to provide various innovative and customer friendly products/services and also to redesign their internal control systems. The data communication network systems play an important role in interface and interconnectivity of banks. With the fast changing technological supported world, banks in India have come a long way. Over the years different methods have been used to transmit data from computer to computer. The data is transmitted by means of data communication media like terrestrial cables, microwave and satellites.

Communication Networks in Banking System

As per the recommendations of the Saraf Committee, the Reserve Bank of India has set up a country wide data communication network for banks linking major centers of the country, known as INFINET (Indian Financial Network) and this network uses satellite communication with very small aperture terminals (VSATs) as earth stations.

VSAT network is a single closed user group network for the exclusive use of banks and other financial institutions. The VSATs are owned by individual banks and the RBI. The hub is owned by the RBI and the Institute for Development and Research in Banking Technology (IDRBT). Satellite services based on VSAT technology can establish reliable links to all sites. The central hub monitors and controls the flow of network traffic.

Internet

The internet is a global network of networks. Computers with internet links can allow users to exchange data, information, messages, files, etc, with other computers across the globe through internet connectivity.

Internet Access Services

Some of the important services available on internet are: E-mail: Most popular and widely used application. Messages can be sent and received to/from any place in very quick time. It is user friendly and cost effective as well.

World Wide Web (WWW)

This facility collates internet related resources and makes available the information. The access to this site assists user to source out a large variety of information. Banks uses internet and web sites (banks' own web sites) to market their products and services. These platforms also allow banks to offer online banking facilities and can be used for posting their financial results and information to customers.

SWIFT

Society for Worldwide Inter-bank Financial Telecommunications (SWIFT) is a co-operative non-profit making organization established under Belgian law with its head quarters at Brussels. SWIFT is wholly owned by its member banks. SWIFT is a paperless message transmission system.

SWIFT – important features:

– Operates on 24x7 basis throughout the year
– All messages are transmitted to any part of the world immediately
– Message formats are standardized
– Information is confidential and is protected against unauthorized disclosure
– SWIFT assumes financial responsibility for the accuracy and timely delivery

SWIFT and banks:

– SWIFT has become an integral part of banking system. SWIFT assist member banks
– SWIFT transmit authenticated financial and non financial messages
– SWIFT with its well-standardized and structured message formats have been offering a reliable system of message transmission
– Banks use SWIFT platform to for transmission of financial and non financial messages covering international finance (settlement of forex deals), international trade (advising of LCs, amendments to LCs etc,)

Clearing House Inter-bank Payment System (CHIPS)

This is a clearing system run by New York clearing house. The financial transactions such as – foreign and domestic trade services, international loans, syndicated loans, foreign exchange trade settlements, are carried out through CHIPS. The CHIPS have a direct interface with the SWIFT system.

Clearing House Automated Payment System (CHAPS)

CHAPS is an automated system set up in UK which ensures immediate settlement of payments.

Clearing House Automated Transfer System (CHATS)

CHATS provide the inter-bank transfer facilities in Hong Kong. CHATS provide same day inter-bank settlement, instant order confirmation and enquiry facilities. The integrity of message transmission is carried out through authentication and encryption techniques.

Banking operations over the years and decades have witnessed many changes and have been adopting from time to time new innovations. The technological revolution especially in the

Information and Technology front has changed the functioning of banks. In today's globalized competitive business environment banks are trying to have the competitive edge by using the latest technology to cut down turnaround time, cut costs and increase efficiency. "e Banking" through many innovative products and services has revolutionized banking operations.

Electronic Fund Management

IT revolution has paved way for banks to implement different systems to handle funds management in banks. This methodology is collectively recognized as Electronic Fund Management.

Electronic Clearing System (ECS)

One of the earliest electronic forms of funds transfer is the Electronic Clearing System. ECS is a retail funds transfer system to effect payments (utility bills, dividends, interest, etc) ECS helps corporates, government departments, public sector undertakings, utility service providers to receive and/or pay bulk payments. ECS is divided into ECS (credit) and ECS (debit)

ECS – important aspects/ features

On receipt of the required mandate, the funds (payments/ receipts) can be handled by a bank through ECS. ECS (debit) is generally used by utility companies like electricity companies, telephone companies and other to receive the bill payments directly from bank accounts of their clients. Instead of payment of utility bills by means of cash or cheque payments, an individual or a company can make payment through ECS. In case the company has the facility of payment through ECS, the client can give a mandate to the company to receive the utility bill amount from his bank account directly. The utility company (service provider) based on the ECS mandate given by the client, would advise the client's bank to debit the bill amount to the client's account on the due date (or on a any date before the due date as per the client's request) and transfer the amount to the company's own bank account. Similarly, ECS (Credit) can facilitate payment to various clients like dividend warrants, maturity values of Annuities.

Real Time Gross Settlement (RTGS)

One of the important IT revolutions in Indian Banking Scenario was the implementation of the Real Time Gross Settlement (RTGS) system by the Reserve Bank of India. With the changing scenario from manual environment to electronic mode, banks started to use faster, safer and efficient methods to transfer funds. In this regard, two important and popular electronic funds transfer systems are Real Time Gross System (RTGS) and National Electronic Funds Transfer System (NEFT) RTGS is an electronic payment system, where payment instructions are processed on a 'continuous' or 'REAL TIME' basis and settled on a 'GROSS' or 'individual' basis without netting the debits against credits. In India, RBI introduced this system and the system is functioning well. The payments so effected are 'final' and 'irrevocable'. The settlement is done in the books of the central bank (RBI). The RTGS system allows transfer of funds across banks on a real time (immediate) basis. Each participant bank needs to open a dedicated settlement account for putting through its RTGS transactions. Not only does it allow transfer of funds, it also reduces the credit risk. Both customers and banks can transfer funds monies the same day at regular intervals within the banking hours.

ECS RTGS

NEFT CBS

ATMs CTs

RTGS:

Special features:
(a) Real Time Gross Settlement helps banks to settle interbank and forex settlements
(b) It also helps banks in handling big ticket funds transfers
(c) Since RTGS it is routed through RBI platform, the credit risk is minimized (this is one of the main advantages in settlement of funds)
(d) Unlike in case of cheque clearance, the drawer of the cheque cannot enjoy the float time (the date of issuance of cheque and the date on which it is received in inward clearing and debited by his banker) However, in the case of RTGS, the remitter's account is debited first and then only the funds are transferred
(e) If all relevant details such as the beneficiary's name, account number, IFSC code of the receiving branch, name of the beneficiary bank, etc., are correctly furnished it would assist the remitting bank to affect the transfer quickly
(f) As the name RTGS suggests, the transfer mechanism works on real time and, therefore, the beneficiary branch/bank should receive the funds immediately. The beneficiary's branch/bank should give credit to the beneficiary's account immediately or latest within 2 hours of receiving the funds transfer message. However, in case the funds cannot be credited for any reason, such funds should be returned to the originating branch within two hours. In such a situation, as soon as the money is returned, the remitting bank should reverse the original debit entry in the client's (remitter's) account. This system is applicable between banks/branches who are on Core Banking Solutions (CBS)

National Electronic Funds Transfer (NEFT)

NEFT is a system similar to RTGS with certain differences. RTGS handles big ticket transactions, whereas NEFT handles smaller size transactions. Most branches are using this facility to transfer funds in an efficient manner.
Once the applicant for the transfer of funds furnishes full and correct details (correct account details means correct name of the beneficiary, the correct account number, the branch and bank of the beneficiary, and the correct IFS code, etc.) funds can be transferred to the beneficiary's account by the remitting bank. Transfer of
funds through NEFT is safe, quick. It reduces the paper work and is cost effective.
NEFT is an innovative electronic media for effecting transfer of funds. Special features of NEFT are:
1. NEFT is a funds transfer system which enables a customer of a bank to transfer funds to another customer of another bank having account with any participating bank
2. NEFT allows both intra and inter-bank funds transfer within a city and across cities
3. Since it is in the form of e transfer, without any physical movement of instruments, funds can be transferred quickly
4. The beneficiary customer gets funds in his account on the same day or at the earliest on the next day depending upon the time of settlement
5. Both the originating and destination bank branches should be on NEFT platform
6. The correct details of IFSC, beneficiary's name, account numbers, etc., should be furnished to the originating bank.
7. The originating bank branch can keep track of the status of the NEFT transaction.

8. In case for any reason the destination branch is not able to afford credit to the beneficiary's account, destination branch/bank have to return the funds to the originating bank within two hours of completion of the batch through which the transaction was processed
9. It is not only easy method of transfer of funds, but also enables the remitters to have user friendly and cost effective transfer of funds

Indian Financial System Code (IFSC)

IFSC is an alpha-numeric code that identifies a bank-branch participating in the RTGS/NEFT system. IFSC has 11 digit code and the first four alpha characters represents the bank, the 5th code is 0 (zero), which is reserved for future use and the last six digits are numeric characters represents the branch. Correct IFSC code is essential for identifying the beneficiary's branch and bank as destination for funds transfers. E.g. Syndicate Bank Cuffe Parade Branch, Mumbai-SYNB0005087

Automated Teller Machines (ATMs)

ATMs are used as a channel for cash management of individual customers. ATMs can be accessed by ATM card, debit or credit cards. To have access the customer (the card holder) needs to use his Personal Identification Number (PIN) issued by his/her banker and access password. ATMs generally used for cash deposit and withdrawals, they can also be used for payment of utility bills, funds transfer thereby ATMs serve as a channel for electronic funds management. Requests for new cheque book and statement of accounts can also be given through ATMs. White Label ATMs- RBI has vide notifications dated 20th June, 2012, permitted non-banking entities to set up or start ATMs which are called White Label ATMs (WLA). From such ATMs customers of any bank will be able to withdraw money, takeout statement, change PIN etc. These WLAs will not display logo of any bank. However, WLA operator has been permitted to display advertisements, and offer value added services as per regulations in force. While WLA operator is entitled to receive a fee from the banks for use of ATM resources by their customers, WLAs are not permitted to charge Bank customers directly for use of WLA.

Internet Banking

Internet banking one of the popular e-banking modes has changed the banking operations and offer virtual banking services to the clients on 24 x 7 basis. It is also called as convenient banking, since the customer (account holder) can have access to his bank account from anywhere at any time, through the bank's web site. The customer is allowed online access to account details and payment and funds transfer facilities. Net banking services of a bank can be accessed through a Personal Identification Number (PIN) and access password as in the case of ATMs. In net banking the advantage for the bank customer is that funds can be transferred from the client's bank account to another account with the same bank or another bank through NEFT/RTGS. Another method of funds transfer facility is online payment of taxes. Bank customer can pay various taxes like income tax, service tax, etc.; Net banking can be used as a channel by the customer to pay the utility bills (electricity bills, telephone bills, etc) on line. Customers can make use of net banking to pay the insurance premiums and similar other payments.

Core Banking Solutions (CBS)

Core Banking Solutions has helped banks to offer better customer service. It has also reduced the time and increased the efficiency. The Core Banking Solutions mainly work on the support of effective communication and good information technology. It is on account of merger of

communication technology and information technology which enables the banks to offer core banking needs of the clients. Core Banking Solutions are computer based banking applications (software) which works on a platform. The computer software handles the different functions of the bank like, recording of transactions, updating the balances in the accounts based on the type of transactions, calculate interests and application of interest, charges etc., The software is installed in the branches and the computer systems are interconnected with a main computer server though communication lines (telephones, satellite, internet, fibre optical) CBS is a back end system, and it processes daily banking transactions and updates the records accordingly.

CBS helps the clients to operate their accounts from any CBS branch. CBS branch assist customers to handle their funds transfers in a quick turnaround time. It also assists the client to withdraw and deposit funds in other branches apart from the parent branch, where he maintains his account.

Data Warehousing- A Data Warehouse or Enterprise Data Warehouse (DWH/EDW) is a database used for reporting and data analysis. It is a central repository of data which is created by integrating data from one or more separate sources. DWH store current as well as historical data and are used for creating trending reports for use by senior management. The data stored in the warehouse are uploaded from the operation systems. The main source of data is cleaned, transformed, catalogued and made available for use by the managers for data mining, online analytical processing and decision support.

Computerization of Clearing of Cheques

Over the years Reserve Bank of India as a facilitator has been playing a vital role in the implementation of innovative systems, to enable banks not only to function effectively but also to offer better customer service. RBI is in charge of the clearing house and clearing operations. It has always taken lead to introduce new systems to speed up clearing process as well to reduce the turnaround time in clearance of funds. Computerization of clearing operations was the first major step initiated by RBI, over the years RBI has been upgrading the system with new changes. To overcome the increasing volume of cheques through the clearing mechanism, RBI has fully automated the clearing house operations. This is based on the Magnetic Ink Character Recognition technology; RBI upgraded the clearing functions with new set of MICR cheques. Under this new system, cheques should have MICR code consisting of 9 digits. Each cheque would have the unique 9 digit MICR code along with the cheque number.

MICR code consists of 9 digits as:

– First three digits indicates CITY {identical to the first three digit of the postal pin code of the CITY (For example: in case of Mumbai, it would be 400)}

– Next three digits represents the Bank and each bank has been given a three digit code called bank code

– Last three digits denote the branch code

Under this MICR system the computer program would read and sort out the cheques based on the codes, thereby, in quick turnaround time, the system is able to handle volume.

Cheque Truncation System (CTS)

Cheques are being used as a medium for exchange of funds, which play a key role in the funds management of customers and banks. The efficient cheque clearing system helps in settlement of receipts and payments. Cheque Truncation is a new system introduced in Indian Banking Scenario. It is a system of cheque clearance and

settlement between banks based on electronic data and/or images without the need for exchange of physical cheques and negotiable instruments like demand drafts, pay orders, dividend warrants, etc. Cheque truncation - Special features:
– Bank customers would get their cheques realized faster
– Quick realization helps in better cash management (receivables/payables)
– In the long run, it would reduce the administrative costs for bank
– Importantly this would assist banks' in reconciliation and also reduction in clearing frauds.

The global e-commerce activities include the interaction of traders (buyers/importers and sellers/exporters) **with** banks and counterparties, manufacturers, service providers etc., Banks across the globe provide payments and settlements services thereby enable the rapid growth of global e-commerce. "e marketing" or cyber marketing is an important segment of e commerce.
Salient features of internet (e) marketing are:

- Internet Interconnectivity Interactivity
- Marketing
- Information Individual Integrity
- Preference

Internet marketing:

Internet based marketing is an important segment in e commerce. It plays a vital role in the supply chain process of exchange of goods between the producer and consumer.
Interconnectivity: Internet is recognized as a network of networks. The search engines assist the user of the internet to have access to required information. For customers, the interconnectivity offered by the internet helps him/her to have information/access to large number of diverse markets. One important feature is that it gives information and access about international markets as well.

Interactivity:

Internet not only allows access but also allows interface and interactivity among users. In view of this interface, it assists both the producer/manufacturer as well as customers to have better communication and choices. It allows the marketer to customize and focus even on individual customers in large markets. On the other hand the customers are also benefitted because of their interface with the marketer, peers and different web sites to make their selection.

Information:

The availability of large number of websites on the internet enables the customers to decide on price, choice of products, designs etc., On account of innovative methods of marketing the customers can have access to information covering wide range of areas.

Individual preference:

The interconnectivity, information and interface provided by the internet network assists the customer with wide choices. Based on his/her preference and capacity a customer can decide on his preference to choose and order.

Integrity:

With the changing time and requirements and on account of security issues and also to safe guard the users from cyber crimes, internet provides tools to check the authenticity of the data and its providers. In view of many fake offers & advertisements, the internet users should be cautious. They should not provide any sensitive information like details of PIN, passwords and

other information to any unauthorized sites, not only to safeguard their interests, but also not to allow cyber criminals to have access to this information.

Internet and Supply Chain Management

Internet also provides online distribution of digitalized products. This helps in quick turnaround reach to a large number of customers, and eliminates the lead time between the place of order and delivery. This also enables a better inventory management and quicker transaction processing. Many enterprises have started using the new concept called Enterprise Resource Planning (ERP) systems. e-distribution (cyber distribution) activities when linked to these ERP systems assist the companies to achieve a greater efficiency in their entire Supply Chain Management.

Cyber Marketing: Limitations:

Internet marketing is also exposed to quite a few problems. Some of them are in-built and others are external problems.

1. Digitization: For cyber marketing, the products should be in digitized format. This process requires manpower, skills and technical knowledge. The digitization is one of the issues faced by e marketing.
2. Shopping experience: Customers especially in India are more used to touch and feel experience as against click and view mode of shopping.
3. Cyber crimes: Despite the popularity of internet and e commerce and e-marketing, on account of different cyber crimes users are concerned about e marketing.
4. Security: While shopping on internet, customers are required to furnish sensitive personal data which are being shared by marketing companies and create inconvenience to the customers and also pose threats to their privacy.

While customers can have faster access to information and details about the range of products, customers are cautioned to be careful on account of various issues and risks associated with cyber marketing.

In today's fast growing e commercial activities, banks' role is very important for the success of global e- commerce. e- commerce should be end to end covering various aspects like from the customer's end, the selection of on line products, placement of orders, and making and settling payments.

An effective global payment channel should be an integral part of global e commerce. Before setting up a global payment channel, an organization should consider certain aspects such as

1. Payment Type: Payments can be made through different modes like credit cards, debit cards, or online transfer. Customers should be allowed to choose any of the method to settle payments. Internal checking and balancing act should be embedded into the system
2. Legal frame work/Regulatory compliance: The system should satisfy the legal and regulatory requirements in the centers
3. Taxes: Taxation laws are different in different countries. The payment system should have the capability to calculate and compute the required taxes, duties as per the local tax laws
4. Banking relationship: Global e commerce involves cross border trade activities and to ensure prompt settlement of payments, the system should be supported by the banks to process these payments. As per the rules and procedures applicable at different centers, the payment system should be supported by well established banks.

5. Risk: Global e commerce is subject to risks. On-line payment risks can be classified into:
Cred it Fraud Repudiation
Credit Risk: The customer may not have sufficient funds to make payment
Fraud: Payments may be made on a misrepresented identify
Repudiation: The customer may refuse to honour payment
Security: Global e commerce is exposed to various cross border nations; hence it is subject to different laws and regulations. Therefore, the payment system should be able to handle the country specific security regulations/guidelines.
An efficient global payment processing system should have the following features;
(i) A single system should enable national and international payments
(ii) It should be able to support multi=currency and multi=payment types
(iii) The processing facility should be active for 24 x 7
(iv) The system should be able to handle the high value transactions
(v) Interface facilities should be available in the system to enable the system in switching to one type of payment to another like (Real Time Gross Settlements (RTGS) Automated Clearing House (ACH)
(vi) Inter connectivity with message switching systems like SWIFT should be part of the system
(vii) It should also be able to handle current and future inflow/outflows
(viii) Importantly, it should have the feature and facility to comply with the regulatory requirements

Risks:

Some of the important risks associated with payment systems are:
Credit Risk: Failure by a party to meet the financial obligations
Liquidity Risk: A party in the system fails to pay on account of insufficient funds
Operational Risk: A risk can arise on account of human error, system failure, frauds etc.
Legal Risk: Non compliance of legal or regulatory framework can create a legal risk
Systemic Risk: It can have a chain effect into the system due to the default of one of the parties

Legal frame work:

The following Acts and Regulations handle the payment and settlement in India:
– The Payment and Settlement Systems Act 2007
– The Payment and Settlement Systems Regulation 2008
– Board for Regulation and Supervision of Payment and Settlement Systems Regulations 2008
International Initiatives: Bank for International Settlements (Basel) has taken many international initiatives to ensure global financial stability. It is also taking actions to strengthen the global financial infrastructure. According to the Committee on Payments and Settlement Systems (CPSS), the core principles for a controlled payments and settlement systems are:
1. The system should be based on a clear legal framework under all relevant jurisdictions
2. All participants should be able to clearly understand the system's rules and procedures. There should be clarity regarding system's impact on each of the financial risks
3. Credit and liquidity risks are important risks in an e-commerce environment. Hence banks Payment systems should cover the area of credit and liquidity risk management
4. Liquidity management depends upon timely settlement of funds. In view of this, banks' settlement systems

should ensure that settlements take place without fail on the value dates (during the day and/or definitely at the end of the day. In case of multilateral netting, at the minimum, the system should be able to complete daily settlements in case the participant of a single big ticket transaction is unable to make the settlement

5. The system should have an integrated high degree of security and operational reliability

6. The system should have a backup system to handle any contingency situations for timely completion of

daily processing

Role of Central Bank in Payment Mechanism

The central bank of a country is responsible in applying the core principles for ensuring that an efficient and cost effective payments system is in place.

The central bank should:

– Clearly define the payment system's objectives and should publicly disclose the role and major policies in respect the payments system

– Ensure that the system is operating efficiently as per the core principles

– As supervisor and facilitator oversee that banks comply with the system's core principles.

– Co-ordinate and co-operate with other central banks for effective implementation of the payments system

RBI as the central bank plays a pivotal role in ensuring that a payment and settlement system is established in conformity with the international standards. Some of the initiatives taken by RBI in introducing different models RBI has been very active in introducing new systems to take care of changing environment and also to safe guard the interest of bank customers, banks, financial instiutions,traders, and others. RBI also ensures that the payment amd settlement systems opreating in India are safe, secure, efficient, accessible and authorised. In addition to the above, RBI played a key role in the establishment of the Clearing Corporation of India Ltd (CCIL), a central organisation that settles transactions relating to government securities and foreign exchange transactions. Over the years, RBI has introduced the above mentioned payment and settlement systems to ensure that the e commerce participants are provided with world class system The success of e-commerce depends upon the efficiency of the support system in timely settlement of funds (payments and receipts). In this regard, the Indian banks are enhancing their payment system to offer international standard service to support e commerce activities.

A simple payment processing model involves the following steps:

(1) Buyer - remitter

(2) Buyer's bank remitting bank

(3) Net Work

(4) Payee's bank (Vendor's bank)

(5) Payee (seller-vendor)

The buyer's bank receives money and instructions to remit the funds. Bank uses its payment and settlement network like RTGS, NEFT and remits the funds to the payee's (beneficiary – vendor – seller's account) (INFINET) INdian FInancial NETwork- INFINET is the communication backbone for the Indian banking and the financial sectors. All banks in the public sector, private sector, co-operative etc. and the premier FIs in the country are eligible to become members of

INFINET. It is a closed user group network for the exclusive use of the member banks and FIs and is the communication backbone for the National Payments System which caters to inter-bank applications like RTGS, Delivery vs. Payment, Automated clearing house, Government Transactions etc. With the availability of better and more reliable technology, INFINET backbone has now been to large extent migrated to multi protocol label switching (MPLS).

Integrated Communication Network for Banks Security and Control Systems

Banks in line with the IT and communication technology revolution and also to maintain better customer relationship management, offer core banking solutions, new on line payment systems like credit cards, debit cards, internet banking services, etc. While this technology based services offered by banks are better and quicker financial services/products, the banking operations are subject to many risks like cyber crimes. Cyber laws through the legal frame work, based on the Information Technology Act, 2000 aimed to setup a sound infrastructure guidelines and rules for e commerce activities through internet. The purpose of IT Act, 2000 is to promote the use of digital signatures for the growth of e-Commerce and e –Governance. It recognizes the digital signature in e-Commerce. The Act allows that any subscriber may authenticate an electronic record by affixing his/her digital signature. IT Act 2000 covers number of aspects relating to e-commerce and several cyber crimes like cyber terrorism, phishing and child pornography.

Digital Certificate and Digital Signature

Digital certificate is an electronic identity provided to an entity by a competent authority or a certification authority. It is a unique public key provided to each entity for establishing the entity's authenticity Digital signatures: As per Sec 2(1) (p) of the Act a digital signature means an authentication of any electronic record by a subscriber by means of an authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the other provisions of the Act

Technological revolutions both in communication and information technology have changed the way of doing business. In today's changed and changing environment electronic commerce and electronic banking has become an integral part of customers as well as bankers. On account of e-commerce and e- banking distances of locations have reduced and many international financial markets have been linked. While it can be appreciated that the computers have become an integral part of one's life, it has also created space for cyber crimes. In view of the fast changing world on account of significant contribution of the IT sector, the cyber crimes pose a significant threat. Cyber crimes are usually carried out by the criminals with technical knowledge and can outstrip and think one step ahead to penetrate into the computers to carry out the crimes.

Cyber Crimes

A cyber crime can be defined as "criminal activity carried out by using computers and internet". A cyber crime can also be defined as "use of computers and/ or other electronic devices via information systems like computer network, internet to handle illegal activities like transfer of funds, withdrawal of funds through unauthorized access" In cyber crimes, computers are either used as tools and/or targets. So the computer which is an electronic devise is used as a medium of cyber crimes.

Effects of cyber crimes:

1. Financial loss 2. Sabotage and theft to identifiable information 3. Exposed to reputation risks 4. Infringement of confidential information 5.Legal consequences 6. Operational risks

Reasons for cyber crimes:

Easy access to data:

If a cyber criminal is able to break into a computer's system, the access to the sensitive data including customer's confidential financial data, information can be copied into a small removable device. Since information technology drives the functioning of corporate, individuals, banks and government departments and other professionals, the storage of unprotected sensitive data and information in their computers pose a significant threat.

Negligence on the part of the users:

Individuals and the employees, officers, executives and other professionals who use the computer systems should be vigilant to protect their information and sensitive data stored in the computers. They should be very careful while using such devices by protecting the access to the system through proper usage of Personal Identification Number (PIN) and passwords. Any negligence on their part would make the cyber criminals' accessto such devices and information easy

Lack of internal control in organizations and banks:

A computer system works based on instructions received from operating systems which are driven by a number of codes. An in-effective internal control and IT audit system would lead to lapses in the computerized environment on account of availability of inefficient hardware systems and software systems. Hence banks should ensure that ongoing internal control and IT audit systems are in place. All software used for operating systems should be preaudited by an IT auditor and certified about their sensitivity, integrity and security. The operating systems should have clear demarcation of access by users at different levels. Since banks use many operating systems for their daily operations for transfer of funds, maintain customer deposit and loan and other accounts, preparation of regulatory returns, financial statements like balance sheets, P&L accounts and other sensitive information and data, allows Core Banking Solutions, use RTGS,NEFT, ECS etc., there should be an effective control to avoid unauthorized access. Hence, the access to the operating systems should have dual control of access based on authorizations.

Classification of Cyber Crimes

Cyber crimes which happen against individuals and others can be classified as under:

Cyber crimes against individuals/ property:

Crimes like cyber harassment, cyber stalking, child pornography, and e mail related crimes. if not controlled can leave undesirable impression on youngsters. The crimes against property (all types) include computer vandalism, IPR violations, Internet time thefts, etc., "Property" in this context not only include computers and/or its components but also refers to software, copyrights, patents, trademarks, and access codes as well. The criminals carrying out these types of crimes, invariably target organizations for various reasons and motives.

Cyber crimes against Society:

Society is one of the important stake holders along with the Government/s. Sensitive websites of governments and the military are subject to hacking. These sensitive web sites are

interconnected and unless otherwise properly controlled and protected, it can pave way for cyber crimes. Crimes like money laundering, sale of illegal and prohibited articles, forgery, etc are examples of crimes against society and government/s.

Some examples of cyber crimes:

– Unauthorized access/control over computer system
– Intellectual Property crimes
– Internet time thefts
– Cyber terrorism against the government or organization
– Distribution of pirated software
– Trafficking
– Pornography (especially child pornography)
– Frauds
– Financial crimes

Individuals
Property
Organization
Society
Cyber Crimes

Financial Crimes

Any crime committed for financial gains is called "financial crime". With the changed banking environment on account of IT and communication revolutions, banks are offering many services like internet and mobile banking, online trading and more of e commerce facilities. Examples of financial crimes are: cheating, credit card frauds, hacking into bank servers, etc.

Fraud and Cheating:

Fraud or cheating can be referred to any dishonest and intentional action to deprive or dupe a person of his or her money, assets or legal rights. As regards cyber crimes frauds and cheating can be classified into:

– *On line cheating and/or fraud:-*

This is the most popular cyber crime. Some examples are

(i) Offer jobs and require you to furnish sensitive information

(ii) Calls for sensitive information like bank account details, credit card details, pass words, user IDs. through the communications purported to have generated from the Income Tax authorities, Government Agencies, Reserve Bank of India and other Institutions

(iii) Informing about winning a lottery or identifying the person as the beneficiary of huge fortunes left by somebody. Such messages are usually circulated from foreign countries.

(iv) Encourage the customer to invest in schemes that offer unduly higher returns

(v) On line shopping may end up in the "buyer buys goods or services" when purchased articles are never delivered.

– *Fraud committed on account of weakness in computer systems-*

Input stage: data is falsified and entered in a manner that makes the data as genuine

Output stage: information is altered and/or destroyed to conceal un authorized transactions. Storage of data is altered or deleted

– *On account of forgery*: Forgeries are committed by using computers. Some examples are: printing of counterfeit currency notes, stamp papers, certificates. Modern printers and scanners photocopiers are used to carry out such frauds.

Information Theft: Information theft arises when confidential information is stolen for various reasons either by intruders to the IT system and /or by insiders. It can result in situations such as (i) the reputation of an entire organization is lost (ii) customer confidential information/data is damaged (iii) regulatory violations are exposed

Other Important Issues

Cyber extortion: A crime involving an attack or threat of attack against an enterprise. It is a crime through which a criminal gains access to a victim's email account by stealing his or her password. By this unauthorized access into the email account, the criminal sends malicious code to various persons in the victim's address book.

Intellectual Property Theft: Intellectual Property refers to the ownership of rights of a person, company with regard to software, copyright, patents, trademark and similar intangible assets. When the ownership rights as mentioned above are deprived partially or completely, it is called as an Intellectual Property Right (IPR) violation.

Computer Security: Computer system is very sensitive to security controls. In case of weak security control, computers are exposed to many risks. On account of carelessness by users, and organizations, the problems would be more including free access to cyber criminals which might lead to financial and reputational loss as well.

Organizations including banks are subject to cyber attacks. Cyber criminals and hackers commit fraudulent acts involving stealing of credit card details of individual cardholders from a bank site. They can make use of the information to defraud the customer and bank to gain financially. If a bank fails to protect or safeguard the sensitive information of the bank and or its customer/s, the bank would face losses which can be broadly classified into:

Financial Loss: Credit card/Debit card information hacked by criminals could result in huge financial loss.

Reputation Loss: On account of weak control system, a bank can face reputational loss

Legal Loss: A cyber attack on a bank can result in legal cases initiated by customer against the bank. The bank might end up paying huge amount of compensation and legal costs.

Banks as financial intermediaries play a crucial role in the financial markets. Banks also act as trustees depending upon situations. It is their responsibility to protect not only the funds of their clients but also the sensitive customer information/data as well. With increasing cyber crimes of different forms, banks should have a very good security control system to protect their customers, bank's assets and other information from cyber crimes.

Integrated Communication Network for Banks Security and Control Systems

Banks are exposed to many risks in their activities relating to management of funds on line banking services. credit card and other e- banking products/services are also facing risks which are associated with the use of IT tools, channels, platforms. Banks should have a good and effective control system to handle IT related issues and risks.

Control system can be classified as:

- Preventive Detective Computer
- Controls Controls Controls
- Detective Internal Information

- Controls Controls System Audit
- Corrective Pysicla Information
- Controls Controls System Security

Preventive Controls: This type of control stops errors or irregularities. Good design/ screen lay out reduces or stops the errors at the time of coding data or entering data from source document.

Detective Controls: Identification of errors or irregularities happens after they occur. For example: An input validation program identifies data input errors.

Corrective Controls: These types of controls remove or reduce the effects of errors and irregularities after they have been identified. If any data is corrupted during transmission the communication software (with inbuilt control) may request for retransmission of information/data.

Physical Controls: In computerized environment, the control of access is very important in view of the confidential and sensitive information/data which are being processed/stored at the data processing center.

Access Control assist the organization and users in restricting entry to authorized persons only to the computer room and also allowing access to computer media, computer components, data, documentation etc. Unauthorized persons should not be allowed to undertake repairs/ maintenance of computer hardware. Access to the computer system should be protected through pass word protection mechanism. Access to the computer system can be allowed by means of PIN, biometric methodology. Access control should be very strict and only authorized users, officers should be allowed inside the data center, computer room and all others should be allowed to enter the data center and computer rooms after recording in the access log.

Output controls: Hard copies of all important reports generated should be preserved properly as per the bank's record maintenance policy.

As part of disaster management, the computer room, data centers need to be checked for proper functioning of fire extinguishers, smoke detectors and other devices. Backup tapes and other data should be stored in off sites.

Regular checks should be carried out to ensure that such back up CDs and other tools/data can be used in case of an emergency/contingency.

Internal Controls: To ensure that the accounting data and other sensitive customer information are accurate and reliable and also to protect assets of the bank, a system of internal controls is built in the computerized systems.

An effective and efficient internal control would assist the bank management to run the bank's operations in a better controlled environment.

Accounting Controls may be in the form of (a) dual controls and authorizations (b) validation checks on data (c) other controls on access to the software applications.

Some other controls include validation of each transaction against limits and balances, stop payments, post dated and stale dated cheques, etc.

Operational Controls: Operational controls are embedded in software whereas access controls can be enforced by the system software and application software at different levels. The operational controls are usually provided in the application software to ensure data integrity and processing. To ensure operational controls, some tools like audit trail, checksum and data encryption are used. Audit trail maintains a record of processes that update the data and

information. Checksum is a number calculated on the basis of certain key information in the system.

Checksum is generated to ensure data integrity stored in a computer file. Data Encryption is the process of systematic encoding of data before transmission to protect the system from unauthorized access, and an unauthorized person cannot decipher it. End to end encryption protects the integrity of data passing between a sender and receiver. In the electronic funds transfer systems, a control mechanism which applies a message authentication code is used to identify changes to a message in transit.

Computer Audit covers, review of operations to ensure compliances of bank's systems and procedures and policies, standards. It includes review of the system's integrity covering fraud detection/prevention, application program and operating system, user acceptance tests at the time of software program implementation and up gradation.

Audit around the computer: The auditor examines the internal control system of the computer installation and related input and output of the application system. 'Around the computer audit' needs to be carried out to ensure/

Verify: (i) the systems are supported by well tested software (ii) a clear cut system generated audit trail is available

(iii) Proper physical controls are in place (iv) duties and responsibilities of various employees are well defined and segregated.

Audit through the computer: This is used to check whether logic and controls are available within the system and records produced by the system are in conformity with the input and expected level of output. Audit through the computers can be carried out by test checks, mock trial runs, and the tools like special audit modules embedded in the application systems to generate audit evidence. Auditors also use audit software consisting of computer program as audit tool. Computer Aided Audit Tools and Techniques (CAATTs) are used to audit computer generated files, records, data and documents. This tool also assists for evaluation of the internal controls of computerized environment in banks.

Information System Audit (IS): This audit is carried out through the IT systems with the assistance of CAATTs and CMITTs. These tools are used to carry out the information system audit. The information system audit covers various controls like preventive, detective and corrective controls and their effectiveness in protecting bank's information systems. Information System audit assesses the strengths and weaknesses of the bank's information system. It identifies the risks of exposure associated with the existing computerized environment. The audit findings can be used as a preventive tool by the banks to take appropriate action to mitigate such risks. IS of a bank can also highlight the following:

– Integrity of the system to safeguard the assets of the bank

– reveals the status of the information system indicating any short comings as well

– assists banks to take a better decision on the management control system of the bank

Off-site Audit

Banks should setup proper offsite monitoring cell (OSM) in audit department or put in place suitable similar structure. Such cell should review the MIS on critical items and sensitize the controlling offices and the branches, for corrective action on daily basis. The OSM cell should also apprise the Top Management of serious irregularities, if any, immediately. The Banks should move to software based audit process.

Information System Security (ISS)

In today's complex and competitive changing business environment, the information technology assists banks across the globe to offer wide range of services and products and also give competitive edge to the players with well supported information system. However, banks are also exposed to many risks on account of growing opportunities on account of information system. This leads to the security concerns of the information system and calls for implementation of an effective control system as well. Since banks are important segment in the financial sector and also acts as trustees of funds. The information system security of banks should provide comfort levels both for the banks as well as customers and regulators.

Objectives of banks' IS Security Policy:

Confidentiality: The confidentiality of customer information and sensitive financial data should not be revealed to unauthorized persons. The IS security should ensure that the confidentiality is maintained

Integrity: Banks' IS security should protect banks information system from accidental or unauthorized and deliberate alteration or deletion of information

All the required controls should be in place to ensure availability of reliable and correct information to the authorized users and persons. These controls include access controls by PIN, pass words, proper approved authentication control, and effective internal controls.

E-banking allows on line banking services and as such the banks' should ensure high level of IS security as part of e banking.

Threats to IS Security: Banks are also offering Core Banking Solutions along with e banking or online banking. In view of these facilities, network security is a concern for banks.

E-mail viruses, Phishing attacks and other issues: Installation of updated antivirus software would assist banks to handle email viruses. The users should be cautioned not to open e mail from unknown sources and spam mails. Phishing is one form of cyber attack in which the attackers make the internet users to reveal sensitive information about the bank account details and personal information. Banks should use certain level of protection by installing fire walls for data integrity. Fire walls do not allow direct access between the internet and the banks' system. This facilitates a high level of control and monitoring. Necessary controls should be exercised in case of computer hardware and software to secure banks information system.

Disaster Recovery Management Control for computer environment: Banks should have in place a disaster recovery policy as part of their management control system. Any incident which results in direct denial or stoppage of essential business functions of a bank for unreasonable period of time is called as a disaster. If this stoppage of business is going to affect the customers it should be treated as disaster. Disaster recovery plan of a bank should give importance to the security of bank's information system. Some examples which cause the disaster to a bank's operations are:

External Factors : Natural disasters like floods, fire and earthquake etc.

Internal Factors : Hardware and Software failures,

Other Factors : virus attack, acts of terrorism

Information Technology Act, 2000 & other Relevant Acts

Information Technology Act 2000 provides legal protection for transactions carried out by means of electronic communication. In view of the recognition given to electronic records,

electronic signatures, and electronic documents, the banks are also required to follow the amendments of other Acts, such as,

(i) The Indian Penal Code 1860
(ii) The Indian Evidence Act 1872
(iii) The Indian Negotiable Instruments Act, 1881
(iv) The Banker's Books Evidence Act, 1891 and
(v) The Reserve Bank of India Act 1934