Information and Communication Technology in Financial Institutions (ICTFI)

THE INSTITUTE OF BANKERS, BANGLADESH (IBB)
DR Tower (12th Floor), 65/2/2 Bir Protik Gazi Golam Dostogir Road, (Box Culvert Road) Purana Paltan, Dhaka-1000
Phone: 02-55112857-60, Fax : (8802) 55112856, E-mail : ibb.diploma@gmail.com
Web : www.ibb.org.bd & www.online.ibb.org.bd

According to the Syllabus of the Institutes of Bankers, Bangladesh (IBB)

Information and Communication Technology in Financial Institutions (ICTFI)

Abul Kashem Md. Shirin
Managing Director and CEO
Dutch-Bangla Bank Limited

Published by the Institute of Bankers, Bangladesh (IBB), December, 2022

Foreword

The Institute Of Bankers, Bangladesh (IBB), established in 1973, has been working for developing the professional skills of the employees of all Banks and Financial Institutions operating in Bangladesh. In this regard, IBB conducts the Banking Diploma examination, JAIBB (Junior associate of the Institute Of Bankers, Bangladesh) and DAIBB (Deplomed Associate of the Institute Of Bankers, Bangladesh) usually held twice in a year throughout the country.

The examinations are being conducted under standard syllabus covering various aspects of Banking profession. As banking is ever-evolving discipline, the syllabus for banking diploma examination is also required to be matched with the changing banking conditions. For the same purpose, A committee was formed under the leadership of Dr. Toufic Ahmad Choudhury former Director General, BIBM and comprising of Mr. Md. Ali Hossain Prodhania, Former Managing Director, Bangladesh Krishi Bank, Mr. Abul Kashem Md. Shirin, Managing Director & CEO ,Dutch-Bangla Bank Ltd, Dr. Mohammad Haider Ali Miah, Former Managing Director & CEO, EXIM Bank of Bangladesh Ltd. Dr. Shah Md. Ahsan Habib, Professor, BIBM, Mr. Alamgir Morshed, CEO, IDCOL, Mr. Omar Faruque , CFCC Head, Standard Chartered Bank and Laila Bilkis Ara, Secretary General, IBB for updating and upgrading the syllabus of IBB Banking Diploma examination.

The committee did the splendid job of formulating the new syllabus for both JAIBB and DAIBB, which was later approved by the Academic Council and Chairman of the institute (Honorable Governor, Bangladesh Bank). The same committee has also been entrusted to formulate standard reading materials by the subject matter specialists and practitioners under their (committee members) guidance in order to facilitate the examinees for consulting focused reading materials instead of so many (sometimes also irrelevant) books. This particular reading material on **Information and Communication Technology in Financial Institutions (ICTFI)** has been prepared and compiled by Mr. Abul Kashem Md. Shirin. We extend our gratitude and thanks to his for taking the trouble of writing the reading material.

All the reading materials of (both JAIBB and DAIBB) will be gradually uploaded in the IBB e- library Web portal. The examinees/ readers/users are requested to send their opinion/ suggestion on any reading material and we will consider their opinion with great importance. Besides, the IBB will modify update the reading materials from time to time as per requirements of the examinees.

Finally, the Institute Of Bankers, Bangladesh takes this opportunity to express its gratitude to the learned members of IBB Council, the syllabus and examination review committee and reading material preparation committee for preparing syllabus and reading materials for IBB diploma examinations.

Laila Bilkis Ara
Secretary General

Table of Contents

6.4.4.3. Cache memory

6.4.5. Special Devices

7. Computer Software:
   - 7.1. System Software
   - 7.2. Application Software
   - 7.3. Programming Language
     - 7.3.1. Low-Level Language
     - 7.3.2. High Level Language
     - 7.3.3. Object Oriented Language
   - 7.4. Database Management System

8. Internet and related terminologies:
   - 8.1. Internet
   - 8.2. WWW
   - 8.3. Hypertext
   - 8.4. Hyperlinks
   - 8.5. Web browser
   - 8.6. Web Page
   - 8.7. Internet vs WWW
   - 8.8. URL
   - 8.9. E-mail

Module-B: Different Approaches to Automation of Financial Institutions (FIs)

1. Data Center (DC), Near DC, Disaster Recovery Site (DRS), Data Center Standards and Certifications
   - 1.1. Data Center (DC)
   - 1.2. Near DC
   - 1.3. Disaster Recovery Site (DRS)
   - 1.4. Data Center Standards and Certifications

2. Computer Networking
   - 2.1. Concept of LAN and WAN
     - 2.1.1. Local Area Network
     - 2.1.2. Wide Area Network
     - 2.1.3. Transmission Media
       - 2.1.3.1. Transmission Media for LAN
       - 2.1.3.2. Transmission Media for WAN
     - 2.1.4. LAN/WAN for Bank
       - 2.1.4.1. Firewall
       - 2.1.4.2. DMZ

3. IT Systems, Storage and Database Backup systems
   - 3.1. IT Systems and Storage
     - 3.1.1. Computer Servers and types
     - 3.1.2. RAID

3.1.3. Clustering
3.1.4. Replication
3.1.5. Dark Fiber
3.1.6. External Storage System
3.1.7. SAN Switch

3.2. Database backup systems

4. FI Computerization approaches
4.1. Stand-alone System
4.2. LAN-based System
4.3. WAN-based System with distributed database
4.4. WAN-based System with centralized database

5. Various Software Systems for FIs
5.1. Core Banking Software
5.2. Switching Software
5.3. Credit Card Software
5.4. Payment Gateway Software
5.5. Software for Mobile Financial System
5.5.1. Mobile Banking System Vs Core Banking System
5.5.2. Mobile Banking system Vs sms Banking system
5.5.3. Available Software for Mobile Financial System (MFS)
5.5.4. Customers of Mobile Banking / MFS and menu items for them
5.5.5. Features of a Software for Mobile Financial Services (MFS)
5.6. Agent Banking Software
5.6.1. Software for Agent Banking System
5.6.2. Agent Banking System Vs Core Banking System
5.6.3. Agent Banking System Vs Mobile Banking System
5.6.4. Type of Devices with Agent Banking System
5.6.5. Security
5.6.6. Available Software for Agent Banking System
5.6.7. Customers of Agent Banking and menu items for them
5.6.8. Features of a Software for Agent Banking Services

Module-C: Alternative Delivery Channels & Funds Transfer Systems

1. Automated Teller Machine (ATM) and Cash Recycling Machine (CRM)
1.1. Services from ATM/CRM
1.2. How ATM/CRM works in case of cash withdrawal?
1.3. ATM/CRM Specifications & related topics
1.3.1 ATM/CRM specification
1.3.2. Denomination available at ATM/CRM
1.3.3. Cash feeding by 3rd party
1.3.4. Partial Dispense of Cash and non-dispense of cash
1.3.5. Capture of money
1.3.6. Network used for connectivity

1.3.7. Card Capture and hot card
1.3.8. One-time and monthly expenditure for an ATM/CRM booth
1.3.10. Income from an ATM/CRM

1.4. ATM/CRM Fraud and remedy
1.4.1. Card Reading Devices
1.4.2. Card-Trapping Devices

2. Deposit Machine

3. Fast Track / Electronic Booth

4. POS terminals
4.1. What is a POS terminal?
4.2. Transaction types supported at POS terminals
4.3. POS Specifications
4.4. How POS works?
4.5. POS terminology
4.6. Fraud at POS and remedy

5. Debit Card, Credit Card, Card technologies and Card Frauds
5.1. Card types
5.2. Terminology for Card transactions at ATM and POS terminals
5.2.1. Issuer and Acquirer
5.2.2. On-us transaction
5.2.3. Off-us or Not on-us transaction
5.2.4. Remote on-us transaction
5.2.5. Interchange fee
5.2.6. Merchant Commission
5.2.7. EMV and Chip Card
5.2.8. Liability Shifting
5.2.9. Charge Back
5.3. International Payment Associations
5.3.1. MasterCard
5.3.2. VISA
5.4. Income from Credit Card Business
5.4.1. Sources of income from Debit Card issuing (payable by cardholder)
5.4.2. Sources of income from Credit Card issuing (payable by cardholder)
5.4.3. Sources of income from ATM acquiring (Payable by cardholder / issuing bank)
5.4.4. Sources of income from POS acquiring (Payable by Merchant / Cardholder)
5.5. Card Technologies
5.5.1. Plastic
5.5.2. Magnetic Strip and Micro Chip
5.5.3. Personalization of bank cards
5.6. Card Fraud
5.6.1. Counterfeit
5.6.3. PIN Fraud
5.6.4. Card Not Present
5.7. Card Fraud Prevention Strategies

9.3.7. Connectivity - sms VS USSD

10. Agent Banking
    - 10.1 History of Agent Banking
    - 10.2 Strategy behind introducing Agent Banking
    - 10.3 Present Scenario of Agent Banking in Bangladesh
    - 10.4 Agent Banking Model in Bangladesh
    - 10.5 Parties involved in Agent Banking
        - 10.5.1 Eligible Criteria for Agents/Sub-Agent
    - 10.6 Agent Banking services in Bangladesh
    - 10.7 Transaction Process at Agent Outlet
    - 10.8 Operational Limits (Regulated by BB) for Agent Banking Customer from Agent Outlet
    - 10.9 Unique selling proposition of Agent Banking
    - 10.10 ROI of Agents/Agent Outlets
    - 10.11 Challenges of Agent Banking

11. Call Center
    - 11.1. What is a Call Centre?
    - 11.2. What is a Contact Centre?
    - 11.3. Difference between Call Centre and Contact Centre
    - 11.4. Mode of Communication in Contact Centre
    - 11.5. Key Components of Contact Centre
        - 11.5.1. Interactive Voice Response (IVR)
        - 11.5.2. Automatic Call Distributor (ACD)
        - 11.5.3. Computer Telephony Integration (CTI)
        - 11.5.4. Call Recording System
        - 11.5.5. Staff (Agent / Supervisors)
        - 11.5.6. Key Performance Indicator (KPI)
    - 11.6. How does the Call Centre / Contact Centre function?
    - 11.7. Types of Call Centre /Contact Centre Service
    - 11.8. Call Centre/Contact Centre Activity Type
        - 11.8.1. Common Inbound Activities
        - 11.8.2. Common Outbound Activities
    - 11.9. Quality Assurance at Contact/Call Centre

12. Systems for sending fund transfer instruction
    - 12.1. Telex
    - 12.2. SWIFT
        - 12.2.1. What is SWIFT?
        - 12.2.2. SWIFT traffic
        - 12.2.3. SWIFT membership
        - 12.2.4. Why to become SWIFT member?
        - 12.2.5. Security at SWIFT
        - 12.2.6. How the SWIFT works?
        - 12.2.7. What are the drawbacks?
        - 12.2.8. User Group in Bangladesh
    - 13.3. Bangladesh Automated Clearing House (BACH)
        - 12.3.1. Bangladesh Automated Cheque Processing System (BACPS)

12.3.2. Bangladesh Electronic Fund Transfer Network (BEFTN)
12.4. NPSB
12.5. RTGS
12.6. CHIPS
12.7. FEDWIRE

Module-D: ICT Security, Cyber Security, ICT Risk Management, Standards, Regulations and Legal Framework

1. ICT Security
    1.1. Business Continuity Threats
    1.2. Internal Threats
    1.3. Mobile Financial Services (MFS) related Risks
    1.4. ATM / POS / e-COM / Card related Treats
        1.4.1. ATM Skimming
        1.4.2. POS Skimming
        1.4.3. ATM Jackpotting
        1.4.4. e-commerce fraud
    1.5. External Risks / Cyber Threats
        1.5.1. Distributed Denial of Service (DDoS)
        1.5.2. Ransomware
        1.5.3. Malware
    1.6. Hacking and Unauthorized Transfer of Money
    1.7. Stealing Credit Card Data
    1.8. Crypto-Currency Threats
    1.9. What to do to minimize the risk?

2. Cyber Security

3. ICT Risk Management

4. Security Standards and Regulations

5. Guideline on ICT Security for Scheduled Banks and Financial Institutions published by the Central Bank of Bangladesh (2015)
    5.1. Categorization of Banks and NBFIs
    5.2. ICT Security Management
        5.2.1 Roles and Responsibilities
        5.2.2 ICT Policy, Standard and Procedure
        5.2.3 Documentation
        5.2.4 Internal Information System Audit
        5.2.5 External Information System Audit
        5.2.6 Standard Certification
        5.2.7 Security Awareness and Training
        5.2.8 Insurance or Risk Coverage Fund
    5.3. ICT Risk Management
        5.3.1 ICT Risk Governance

- 5.3.2 ICT Risk Assessment
- 5.3.3 ICT Risk Response

5.4. ICT Service Delivery Management
- 5.4.1 Change Management
- 5.4.2 Incident Management
- 5.4.3 Problem Management
- 5.4.4 Capacity Management

5.5. Infrastructure Security Management
- 5.5.1 Asset Management
- 5.5.2 Desktop/Laptop Devices Controls
- 5.5.3 BYOD Controls
- 5.5.4 Server Security Controls
- 5.5.5 Data Center Controls
  - 5.5.5.1 Physical Security
  - 5.5.5.2 Environmental Security
  - 5.5.5.3 Fire Prevention
- 5.5.6 Server/Network Room/Rack Controls
- 5.5.7 Networks Security Management
- 5.5.8 Internet Access Management
- 5.5.9. Email Management

5.6. Access Control of Information System
- 5.6.1 User Access Management
- 5.6.2 Password Management

5.7. Business Continuity and Disaster Recovery Management
- 5.7.1 Business Continuity Plan (BCP)
- 5.7.2. Disaster Recovery Plan (DRP)
- 5.7.3 Data Backup and Restore Management

5.8. Acquisition and Development of Information Systems
- 5.8.1 ICT Project Management
- 5.8.2. Vendor Selection for System Acquisition
- 5.8.3 In-house Software Development

5.9. Alternative Delivery Channels (ADC) Security Management
- 5.9.1 ATM/POS Transactions
- 5.9.2 Internet Banking
- 5.9.3 Payment Cards
- 5.9.4 Mobile Financial Services

5.10. Service Provider Management
- 5.10.1 Outsourcing
- 5.10.2 Service Level Agreement

6. PCI-DSS, BS7799 and ISO 27000

6.1. PCI-DSS
- 6.1.1 What is PCI DSS?
- 6.1.2. PCI DSS certification
- 6.1.3. PCI DSS Compliance levels
- 6.1.4. PCI DSS requirements
- 6.1.5. Understanding PCI DSS compliance levels

6.2. BS7799

6.2.1. What is BS7799?
6.2.2. History of BS 7799
6.2.3. BS7799 vs ISO 17799
6.2.4. Who must comply?
6.2.5. BS7799: Part-I: Security Domains, Objectives and Controls
6.2.5.1. Domain-1: Security policy
6.2.5.2. Domain-2: Security organization
6.2.5.3. Domain-3: Asset classification and control
6.2.5.4. Domain-4: Personnel security
6.2.5.5. Domain-5: Physical and environmental security
6.2.5.6. Domain-6: Communications and Operations Management
6.2.5.7. Domain-7: Access control
6.2.5.8. Domain-8: Systems development and maintenance
6.2.5.9. Domain-9: Business continuity management
6.2.5.10. Domain-10: Compliance
6.2.6. BS 7799: Part-II: ISMS and Certification
5.2.6.1. Compliance/Certification Process
5.2.6.2. What is an ISMS?

6.3. ISO 27001
6.3.1. Benefits of implementing an ISMS
6.3.2. What are the 14 domains of ISO 27001?
6.3.3. How many controls are there in ISO 27001?
6.3.4. What is "ISO 27001 certified"?

7. Legal Framework in Bangladesh
7.1. Cyber Law
7.1.1. What is Cyber Law?
7.1.2. Cyber Crime Categories:
7.1.3. Cyber Crimes Activities:
7.2. ICT Act
7.2.1. Introduction
7.2.2. Applicable fields of ICT Act-2006
7.2.3. Objectives
7.2.4. Selected clauses

Module-E: Document Handling Systems, Additional Banking Applications & Other Aspects

1. Cheque Processing Systems
1.1. Clearing and Settlement Systems
1.2. Conventional Cheque Clearing Process
1.3. MICR (Magnetic Ink Character Recognition)
1.4. Cheque Truncation
1.5. RTGS (Real Time Gross Settlement)
1.6. BACH (Bangladesh Automated Clearing House)
1.6.1. Bangladesh Automated Cheque Processing Systems (BACPS)
1.6.2. Bangladesh Electronic Funds Transfer Network (BEFTN)

2. Additional Banking Applications
    2.1. ERP Software
        2.1.1 What is ERP System?
        2.1.2 Components / Modules of an ERP Software:
        2.1.3. Components of an ERP System
        2.1.4. ERP advantages and disadvantages
        2.1.5. Renowned ERP Software:
            2.1.5.1. SAP ERP from SAP
            2.1.5.2. PeopleSoft ERP from Oracle
    2.2. CRM Software
        2.2.1. What is CRM?
        2.2.2. Fields of application:
            2.2.2.1. Sales force automation
            2.2.2.2. Marketing
            2.2.2.3. Customer service and support
            2.2.2.4. Analytics
            2.2.2.5. Integrated/Collaborative
        2.2.3. Software for CRM
    2.3. E-mail software
        2.3.1. What is e-mail?
        2.3.2. Operation Overview:
        2.3.3. Components in a messaging system:
        2.3.4. Popular E-mail System:
            2.3.4.1. Sendmail:
            2.3.4.2. Qmail:.
            2.3.4.3. Microsoft Exchange Server:
            2.3.4.4. Lotus Domino:
        2.3.5. Licensing of commercial product:
            2.3.5.1. Exchange Server:
            2.3.5.2. Lotus Domino:
    2.4. Anti-Virus software
        2.4.1. What is antivirus software?
        2.4.2. How Antivirus works?
            2.4.2.1. Signature based detection:
            2.4.2.2. Behavior Based Detection:
        2.4.3. Licensing:
        2.4.4. Popular Antivirus programs:
    2.5. Anti-malware software

Module-F: FinTech, Artificial Intelligence and future technology based banking

1. FinTech, RegTech and TechFin
    1.1. FinTech
    1.2 TechFin
    1.3 RegTech

2. Basic Crypto Currency and Block Chain Technology

Module-A

Introduction to ICT and Computer Systems

1. Information and Communication Technology (ICT)

1.1. What is ICT?

Information and Communication Technology (ICT) is a technology which refers computer systems (such as computer hardware & storage), software (such as applications and databases) and systems for communication of information (such as networking devices and technologies) that combined allow people and organizations to interact in the digital world.

1.2. What is Computer?

As per definition given by C.S. French, a Computer is a device which can accept data, process data and output data. In other words, Computer is a machine which is controlled by some programs, accept data as ***input***, ***process*** them and finally submit result or required information to the users as ***output***.

For example, customers make deposit and withdraw money from Banks. The amount deposited or withdrawn is inserted by a Bank Teller into the Computer as *data*. Now Computer *processes* the data which includes updating customers balance in the Customer Ledger. At the day-end the Computer generates "Balance Listing" and "Statement of Affairs" which is called *information* or *output*. Based on the *output* or *information*, the users and management undertake important decisions.

Figure: Laptop Computer

However now-a-days, the Computer is used in many other ways such as for e-mailing, browsing, playing games, listening music, viewing video and TV, making a phone call etc.

1.3. What is Information Technology?

In short, the Information Technology is known as IT. As per C.S French, the Information Technology (IT) is the technology which supports activities involving the creation, storage, manipulation and communication of information, together with their related methods, management and application.

Information Technology not only limits to the processing of information, but also works with communication of information, and as such this term is extended to information and communication technology (ICT). All the process and systems needed to capture, store, process and communicate information is collectively called Information Technology.

1.4. Importance and use of ICT

Use of Information and Communication Technology (ICT) in Banking has brought a revolutionary change in the customer services. The features of the ICT for which it contributed much in the financial services are discussed below:

a. High speed:

Computer can work with very high speed. A computer can complete a 100 year's work of a man in a few minutes only.

In 1980s, there was no ICT in use in Banking sector in Bangladesh. Thus Bankers used to maintain a manual ledger. When a customer came to the counter for withdrawal of money, first the Teller had to check the signature manually and make a manual entry into a large ledger and then hand over money to the customer. This took long time and thus customers had to stay in queue for hours together. After introduction of ICT in Banks, the posting in computer-based ledger became an activity of a minute only, and as such quick customer service became possible. On the other hand the day-end, week-end, month-end and year-end activities such as calculation of interest, income-expenses, and preparation of financial reports including trial balance, balance sheet, statement of affairs and income-expenditure report were a nightmare job for the bankers. However after computerization, these activities are done by the computer in an hour and all the Bankers were set free. Thus the Bankers were able to give much attention in other activities such as business development.

b. Available *anytime*:

Before introduction of ICT in banking services, the customers had to complete all the transactions before a set time in working days only. Now a customer can avail the banking services 24 hours a day, 365 days a year. A customer can use ATM for withdrawal of money *anytime*. The computers in the Bank's data center are in running mode all the time and thus can update the customers balance instantly. The bankers on the other hand can obtain all the activity reports (such as who has withdrawn money, what is the amount and from where he has withdrawn etc.) in due time. Using the Internet Banking system, a customer can do banking from his office or house *anytime*. Customers can buy goods and services from a shop and pay bills online using his debit or credit card and POS terminal installed at the shop *anytime*. A customer can also use his mobile phone and do some transactions *anytime*.

c. Available *anywhere*:

Before introduction of ICT in banking services, a customer had to go to a branch physically for obtaining banking services. Now the customer can avail the banking services from anywhere he desires. Not a matter where he has opened his account, he can go to any branch and avail full range of banking services. He can go to an ATM in any city and withdraw money, check balance, print mini statement, deposit money and pay

utility bills. The customer can go to any shop in any city of the world and buy goods and services using his International Credit or Debit Card. He can also access his account through internet from any part of the world.

d. Accuracy:

Computer (a component of ICT) can work with 100% accuracy if the program and data supplied is correct. “Garbage in garbage out” is very true for the computer. Computer can never be incorrect. However it can give wrong result if the data is wrong or the programming logic is incorrect. If a customer withdraws Tk.100/- and the Teller during posting in the computer, types Tk.1000/- instead of Tk.100/-, customer’s balance will be updated wrongly. This is not an error for the computer as the data was provided wrongly.

e. Memory:

Computer has a very huge memory – it can store and process a large number of data. Its storage is more than the storage of a big library. It can store customer data for several years. The computer can retrieve the data from the storage very quickly and accurately.

f. Diligence:

Computer can work continuously for a long time without tiredness which is not possible for a man. A computer server in a Bank starts once and never stops for years together. Thus non-stop 24/7 service is possible for banking products such as ATM, POS terminals, Internet Banking, e-commerce etc.

g. Interfacing:

Interfacing is the way of communicating one system with another system of ICT such as communicating IT system of one bank with that of another bank. Thus a customer of ‘May Bank’ of Malaysia is able to withdraw money from the ATM of Dutch-Bangla Bank in Bangladesh using his Visa or MasterCard. On the other hand a customer of Dutch-Bangla Bank can pay shopping bills at a shop in USA using his MasterCard or Visa Card.

2. Electronic Banking and Online Banking

2.1. Electronic Banking

Electronic Banking is modern banking techniques using which a Bank customer can avail banking services without going to a bank branch physically and without assistance of any bank officials. The electronic banking services are narrated below:

2.1.1. ATM

ATM or Automated Teller Machine is used mainly for withdrawal of cash by a bank customer using his debit, credit or prepaid card. Besides, the ATM allows the card holder to receive the information on the current status of his account (including an extract on a paper), and also to transfer money from one account to another.

ATM is supplied with the device for reading a card, and with a display monitor and a keyboard for interaction with the card holder. The ATM is equipped with a personal computer which communicate with a central server of the bank for checking PIN, updating account balance and finally instructing the cash dispenser to dispense cash.

Figure: An Automated Teller Machine

The cash dispenser is a storehouse of cash. Monetary denominations in an ATM are placed in cassettes which are placed in a special safe (vault). The number of cassettes defines the number of the denominations which are given out by an ATM.

For maintenance of communication functions ATMs are equipped with LAN Card.

Banks in Bangladesh have installed ATMs in different parts of the country with a view to pass on the banking services close to the customers. As such the customers do not need to go to bank branches for withdrawal of money or other services. He can avail these services from an ATM installed close to his residence, office or shopping place. ATMs remain open 24 hours a day and 365 days a year. In this way the customers can withdraw or deposit money through out whole day and night even in the holidays. This has given freedom of banking to the customers. Now customers are not worried to withdraw money before close of cash counter at 3:00 pm or before a long holiday or before a journey to another city.

Bank customers can avail following services from ATM Network:

a) Cash withdrawal
b) Payment of utility bills
c) Fund transfer from customers own account to another account in the same bank or with another bank
d) Checking account balance
e) Printing mini statement (last 5 transactions).


Figure: A factory is manufacturing ATMs. Vaults and dispensing units are seen in the picture.

ATM booth is a place where one or more ATMs are installed by a bank. In some ATM booths a separate deposit machine has been installed to accept cash in envelop and cheque which is called **Cash Deposit Machine (CDM)**. In such case customer inputs his account number and amount to be deposited in the deposit machine. The machine opens its door and the customer drops the envelop into the machine. In this way of depositing money, banks sometime may found that the amount in figure inputted into the system and the money actually deposited using envelop is not matching. This may create a dispute. Bank normally count such money inside the envelop under the surveillance of a CCTV system to record such anomalies if any.

There are ATM machines which can accept bundles of money, count the money supplied in different denominations and check for fake notes. Additionally these ATMs can deliver the same money received from one customer to other customers who come to the same ATM later on for withdrawing money. These types of ATM machine are called **cash-in cash-out ATM or Cash Recycling Machine (CRM)**.

To avail the ATM services by a customer, he needs a plastic card and PIN (Personal Identification Number). This plastic card and PIN is supplied by the bank to the customer after opening an account with the bank. This plastic card is called as ATM card or Debit Card. The customer first inserts his card in a slot at ATM and then type his PIN using the keyboard of ATM. Then a menu appears using which the customer can do the required activities. In addition to the ATM card or debit card, a customer can also use his Credit/Prepaid Card and PIN for withdrawing money from ATM.

2.1.2. POS terminal

A typical POS (Point of Sale) terminal has built-in devices for reading microchip and magnetic strip from a card, key board with a built-in PIN PAD, a printer, a port for connection with a PC or with an electronic cash register (ECR). Besides usually the POS terminal is equipped with a modem with a capability to dial to the NAC (Network Access Controller) at Data Center of the Bank.

Modern POS terminal have GPRS functionality, thus instead of modem it contains a SIM card for connection with the data center using mobile connectivity. Thus this type of POS terminal is movable. To support the mobility of the POS terminal, it has been provided with a battery for supplying power during transactions. The advantages of the GPRS POS terminals are as follows:

a) The merchant does not require a PSTN connection for use of the POS terminal.

Figure: A PSTN POS terminal

b) The customer does not require to handover the card to the merchant which can lead the card to be duplicated.
c) The customer does not require to come to the cash counter for insertion of his PIN at the PIN PAD of the POS terminal.
d) It can be used by a small floating shops who sales the goods in different places such as residences, parks, rail stations etc.

Banks buy the POS terminals and supply to a merchant (shop/restaurant) free of cost but at an agreed merchant commission. The merchant commission refers to the commission in percentage over the sale amount settled using the supplied POS terminal which the merchant pays to the bank. This normally rages from 1.0% to 2.0%. As per the agreement a merchant should not charge the customer for the commission amount. If a merchant does so, the bank has the right to withdraw the POS terminal from the merchant.

After selection of goods from a shop, a customer comes to the counter and handover the card to the teller for settlement of the bill. If the card is a meg-strip card, the teller swipes the card at a long slot or if the card is a chip based card, the teller deep (insert) it into a slot. The teller types the billed amount and asks the customer to insert his PIN and the customer types his PIN on the key board. Then the teller presses OK button. The POS terminal automatically dials to a stored number and gets connected to the data center of the bank. It then transfers the card information with amount to the bank server for debiting the customer account and crediting the merchants account. If the server can perform the operation successfully, it informs the same to the POS terminal, and the POS terminal prints an approval slip at its printer.

2.1.3. Internet Banking

Internet Banking is a way of performing some banking activities through internet by a customer himself sitting at his home or office. In some other country, this is also termed as Online Banking. For accessing the internet banking facility of a bank, the customer must have a computer or smart phone and an internet connection. Then he needs to get an ID (identification) and corresponding password from his bank for accessing internet banking system.

Having all the above, the customer first visit to the website of the bank (by typing website address of the bank at the address bar of a browser) and click the link written “Internet Banking”. The internet banking page will be displayed where the customer has to type his ID and password. If these are correct, the customer will get a menu using which he can perform the following activities:

a) Check balance of accounts
b) View and print the account statement for a particular period
c) Payment of utility bills
d) Recharge any mobile phone
e) Payment of loan installments

f) Payment of fee of the educational institutions
g) Add / modify / delete Standing Instruction
h) Open a FDR debiting money from his SB / STD / CD account
i) Redeem FDR at maturity or before maturity (money will be transfer to SB / STD / CD account)
j) Creating LC and sending to the Bank for authorization
k) Sending request for Cheque book
l) Making stop payment on a cheque leaf
m) Check status of a cheque deposited for clearing
n) Apply for a personal loan
o) Checking interest rate
p) Checking exchange rate
q) Change password, etc.

It may be mentioned that using internet banking system, a customer can't receive or deposit cash.

2.1.4. sms Banking

sms banking is a way of performing some banking activities by a customer himself by sending sms from his mobile phone. For accessing the sms banking system, the mobile of the customer must be registered with the bank. The bank will provide a PIN to the customer. Then the customer can perform the following activities by sending sms from his registered mobile:

a) Checking account balance
b) Obtaining a mini statement of his account
c) Payment of utility bill
d) Payment of bill against purchase of goods and services
e) Mobile top up
f) Fund transfer
g) Change PIN etc

To do any of the above activities, the customer has to write a sms as per the syntax defined by the bank. For example, for checking account balance the customer may write: "Bal 1234", where 1234 is his PIN. Then he sends the sms to the short code of the bank, say 14214. This will first go to the mobile operator's system which knows that the short code (14214) belongs to a bank. The mobile operator will send his sms along with the mobile number to the bank server. As the key word is "Bal", the bank server knows that the customer is looking for his account balance. System will find the corresponding account number (against the mobile number), extract the balance of the account (if the PIN is correct) from the database and send a sms including account balance to the mobile of the customer. The return sms may be as under:

Date: 30/5/2010, Time: 2310, Account No.: 99999999, Balance: BDT 9999.99

The syntax for other activities may be as under:

i) Mini statement: stm <PIN>
ii) Utility bill payment: ub <PIN> <biller code> <amount>
iii) Payment against purchase: pay <PIN> <merchant code> <amount>
iv) Mobile top up: tu <PIN> <mobile number> <amount>
v) Fund transfer: ft <PIN> <to account number> <amount>
vi) Change PIN: pin <old PIN> <new PIN>

2.1.5. Alert Banking

Alert Banking is a system which sends a sms to the customer when a debit or credit transaction occurs in the customer's account. For example if the monthly salary of Tk.27,000/- of a customer is deposited into his account, system will generate a sms as under and send to the customer's mobile registered for this service:

"Your account has been credited for an amount of BDT 27000/- on 23/4/2010 at 2310."

Alert Banking useful for the customers as he can come to know about any fraudulent activity in his account instantly and can undertake immediate measures.

To setup an alert against an account, the bank needs to know the following from a customer:

a) Mobile number of the customer
b) Account number of the customer
c) Debit amount: If the transaction amount is more than this, a debit alert will be generated. Normally this is set at zero.
d) Credit amount: If the transaction amount is more than this, a credit alert will be generated. Normally this is set at zero.

2.1.6. IVR

IVR or Interactive Voice Response is an automated system where a customer can call from his land phone or mobile phone and interact with the machine pressing digits to perform some banking services. These services may include obtaining information such as balance inquiry or do transactions such as fund transfer and activate/deactivate a debit, credit or prepaid card.

To do banking through IVR, the customer needs to obtain a T-PIN from the Bank. Then the customer will call to a short code such as 3225. The call will be terminated to a machine in the bank. The machine will welcome the customer and ask "Press 1 for account services, 2 for Card services ……" Now if the customer presses 1 in the keyboard of his phone device, the machine will ask "Press 1 for account balance, 2 for fund transfer, 3 for cheque book request, 4 for exchange rate, ….." If the customer now presses 1, the system reads-out his account balance.

2.2. Advantages and disadvantages of Electronic Banking

After introduction of the electronic banking systems, it has been a revolutionary change is the way of doing banking both by the bank officials as well as its customers. The Bank officials do not need to record all the transactions manually. The customers do not need to be in long queue at the branches. The advantages and disadvantages of electronic banking systems are mentioned below:

2.2.1. Advantages:

i) Customers do not need to go to a branch for withdrawal of money. He can go to any ATM in the city he lives or in another city and can easily withdraw money.

ii) Customers do not need to withdraw money during office time. He can withdraw money from ATM at any time, such as during day or night, even on a holiday.

iii) If a customer goes for a personal / official / business tour, he does not need to carry huge amount of money with him. Thus the risk of hijacking / theft of money can be avoided.

iv) Customers do not need to go to branch for payment of utility bills and face a long queue. The customers can pay his utility bills such as electricity bill, telephone bill, gas bill and tuition fees of the educational institutions using ATMs anytime anywhere, using internet banking system from home, office or while travelling abroad, and using sms & IVR systems 24 hours a day, 365 days a year from home, office or while the customer is on a vehicle.

v) The customer does not need to go to a branch for transferring money from his account to another account. He can affect such fund transfer anytime from anywhere using ATM, Internet Banking system, sms system or IVR system.

vi) Using internet banking system, the customer can open an FDR debiting his SB/STD/CD account. The FDR will be redeemed or reinvested at maturity as per the instruction. If required, the FDR can also be redeemed before maturity.

vii) The customer does not need to go to a market with a huge amount of money. He can use his card at the POS terminal to pay his bills. This reduces risk of carrying fund. On the other hand, the shop owners also do not need to keep huge cash at his counter which in turn reduce risk of theft at counter or hijacking during transferring money from the shop to the bank.

viii) If the customer is a salary holder, he gets an alert message at the time of depositing salary into his account. Thus he always remains updated on the status of his account.

ix) If a foreign remittance is deposited in the account of a customer, he gets an instant sms at his mobile phone which informs him on the remittance amount. Thus customer does not need to remain worried about the status of the remittance sent by his near and dear ones from abroad.

x) If any unusual transaction happens in his account, he can come to know the same instantly and make complaint to the bank in time. He can also inform the bank to take necessary measures to avoid such fraudulent activities in his account / card in future.

xi) After introduction of electronic banking systems, most of the customers perform banking activities by themselves. Thus the bank officials can invest their time for other activities. Bank can serve more customers using lesser employees.

xii) Customer has more control over his deposited money.

xiii) For electronic banking services, the per-transaction cost is minimum. As such the bank can charge small amount of fees to the customers for such services.

xiv) As the customers have better control over his money and the money is available all the time anywhere, the customer keeps all the deposit to the bank offering electronic banking services. As such the low cost deposit of the bank increases and consequently the profit of the bank also increases.

2.2.2. Disadvantages:

i) Customers can not withdraw more than an amount and more than a number of times from the ATM. For example, a particular bank may set the amount per withdraw at Tk.20,000/-, total withdraw per day at Tk.50,000/- and number of time the customers can withdraw per day at 5. If the customer requires more than Tk.50,000/- in a day, he must go to a branch.

ii) Customers may not get money from ATM due to fault at ATM hardware or software or due to exhaust of the money at the ATM vault.

iii) Cash can’t be withdrawn or deposited through Internet Banking, POS terminal, sms or IVR systems.

iv) Customer must have a computer with internet connection to access internet banking system.

v) If a hacker can know the password of the Internet Banking System of a customer, he can transfer money to another account and then withdraw from ATM.

vi) If a hacker can capture the PIN and card information of a customer during travelling the information from ATM/POS to the bank data center, he can produce a duplicate card and withdraw all the money of the customer from an ATM. Hacker can also install a skimming device in the ATM and collect the card information and PIN.

vii) sms is not a secured media of communication. As such banking activities using sms is not secured.

viii) Electronic Banking systems are technology driven. Thus the customers need to know some basic technology-driven operations.

ix) Bank needs a large set of skilled manpower for installation and maintenance of electronic banking systems.

x) Setup and ongoing maintenance of electronic banking systems are very costly.

2.3. Online Banking

In some of the countries, the online banking refers to the Internet Banking System. However in our country, online banking means installation of a centralized core banking system in which all the branches are connected using a WAN (wide area network) and thus the customers can do banking in any branch of the bank. This is also termed as “Any Branch Banking”. The advantages and disadvantages of online banking or Any Branch Banking are as under:

2.3.1. Advantages

i) If the online banking system is introduced in a bank, the customer of a branch becomes customer of the bank. Thus he can withdraw money from any branch or deposit money to any branch of the bank. He can also perform all the transactions from any branch of his choice such as balance inquiry, collection of account statement, placing request for cheque book, collection and preparation of Payment Order (PO) or Demand Draft (DD), opening of LC, buying/selling of foreign currency, receiving foreign remittance etc.

ii) If a customer goes to another city for personal / official / business purpose, he does not require carrying money with him. He can withdraw money from a branch in that city.

iii) If a customer receives money from his business partner while he is travelling another city, he does not need to carry back all the money with him. He can deposit the money to any branch of the bank in that city.

iv) The customer does not need to send PO or DD to other parties for business purpose. He can directly deposit money to the account of his business partners.

v) In the online banking system, all the customer information and transactions are stored centrally in a data center. Thus it is not required to maintain huge infrastructure and IT experts in each of the branches.

vi) Due to installation of core banking system in banks, it has become possible to debut various delivery channels such as ATM network, POS network, internet banking system, sms banking system, alert banking system, IVR system etc.

2.3.2. Disadvantages

i) For introducing online banking system, all the branches need to be brought under a WAN (wide area network). Required communication infrastructure for WAN is not available in all area of the country.

ii) After introduction of online banking system, all the banking activities become dependent on computer. Therefore if there is no electric power for a long time, all the banking activities become unavailable for that period. This becomes a challenge for the online banking system in the rural area where availability of electric power is very rare.

iii) For operation of online banking system, all the employees of a branch must be computer literate.

iv) Sometime, the communication network fails (break down). In such case the branch become disconnected from the data center and thus unable to do any transaction. This creates suffering to the customers.

v) Preparation of central data center, installation of core banking software, setup of WAN and supply of computers to all the branches for each of the employees are very costly.

vi) Setup and maintenance of online banking is a very complex activity. For this a very strong expert IT team is required. Such a team is not easily available. They are also very costly.

vii) Cost of centralized software is much higher than that of a de-centralized software.

3. Mobile Financial Services:

Mobile Financial Services (MFS) is a banking system for mainly unbanked population using which a registered mobile holder can deposit (cash-in) & withdraw (cash-out) money from an agent, transfer money from his MFS account to another MFS account (P2P), receive foreign remittance from abroad, pay shopping bills (Merchant Pay) & utility bills (Bills Pay), receive salary & various government allowances & stipends, and recharge airtime for his own/relatives mobile etc.

Payment of shopping bills is a P2B (person to business) activity which is also called as Merchant Payment. Using this function of MFS, the customer can buy goods and services from a shop or restaurant (called merchant) and pay bills by transferring money from his mobile account to the merchant's mobile account.

At the start of MFS in Bangladesh in the year of 2011, only 13% of the population was maintaining bank account while 45% were owner of a mobile phone. Thus it was thought that using a mobile banking technology, a huge unbanked population could be brought into the banking system. The banking activity could also be extended to the rural areas where there was no presence of bank. This would also stop informal remittance both local and foreign.

Accordingly, NOC was given by the Bangladesh Bank to Dutch-Bangla Bank and Brac Bank to start mobile financial services pending formulation of guideline and related policies under which a proper license could be issued. Dutch-Bangla Bank started its MFS titled "Rocket" in March, 2011 and Brac Bank in June, 2011 in the name of "bKash". Then other banks started their own MFS services one by one. The most recent MFS are "Nogad" of Bangladesh Post Office and "TAP"of Trust Bank and Robi, a mobile operator in Bangladesh.

Later on the Bangladesh Bank formulated MFS policy under which licenses were granted to the MFS operators. According to the existing policy in force, the MFS model in Bangladesh is Bank-led which means that in the MFS, a bank should maintain at least 51% share.

After 11 years of journey of the MFS in Bangladesh, it is the 2nd largest MFS market in the world after Kenya. As per the report of Bangladesh Bank, present (as of Feb, 2022) number of registered clients in the MFS are 81.86 million out of which number of active clients are 27.08 million. Around 10 million Agents are providing services to these clients. Total number of transactions held in Feb, 2022 (for a month) is 226 million and total amount of transaction during this period was Taka 413 billion. The Taka 413 billion transactions included the following:

1. Cash-in transactions: 146 billion
2. Cash-out transactions: 137 billion
3. P2P transactions: 98 billion
4. Salary disbursement: 11 billion
5. Merchant Payment: 5.8 billion
6. Utility bill payment: 4.4 billion
7. Government Payment: 2.8 billion
8. Inward foreign remittance: 0.3 billion
9. Others (including recharge): 7.7 billion

4. Agent Banking:

Performing Core banking activities is complex for the rural uneducated clients as they can not write and sign a cheque which is required for withdrawing money from their respective bank accounts. They also can't remember and input PIN of their debit card for withdrawal of money from an ATM.

On the other hand, they require PIN to be submitted using their respective mobile phones in case of withdrawal of money from their respective mobile banking account (MFS account) which they can't remember and type in a mobile phone. As such mobile banking also not suitable for rural uneducated clients.

To overcome these problems, the concept of Agent Banking was initiated by the Central Bank of Bangladesh in 2015 where all the transaction will be authorized by pressing finger prints in a device. All kinds of banking transactions except foreign exchange transactions are allowed in Agent Banking. Agent outlets are licensed by the respective banks in the rural area which on behalf of the bank perform the transactions. Agents get commission on deposit amount (float amount), account opening and various transactions including disbursement of foreign remittance and recommendation of credit facilities. The agents in their respective outlets can only perform transactions of a specific bank and they are not allowed to perform any other business in the outlet.

The current status of Agent Banking in Bangladesh is given below (as on 31 June, 2022):

Particulars	As on 30 June, 2022
No. of Banks with License	30
No. of Agent Outlets	19,737
No. of Agent Banking Accounts	16,074,378
No. of Female Accounts	7,937,867
Number of Rural Accounts	13,890,321
Amount of Deposits (in BDT million)	280,853
Amount of Loan Disbursed (in BDT million)	76,456
Amount of Inward Remittance (in BDT million)	970,481

Ref: Bangladesh Bank

5. e-Commerce and m-Commerce:

5.1. e-Commerce

According to James A. O'Brien "e-commerce is the buying and selling, and marketing and servicing of products, services and information over a variety of computer network. In short, buying and selling of goods and services over internet is called e-commerce.

In this system, the seller (merchant) develops a website where he displays all the items he wants to sale. Each item will have one or more pictures, description, specifications and area based delivery time. The customer visits the website and selects the items he wants to buy. The selected items accommodated in a place which is called cart. When the selection is finished, the buyer enters the deliver address (if not registered earlier) and presses “Check-out” button to pay the bills.

The merchant’s website is linked to an e-commerce system of a bank. The e-commerce system of the bank is known as “payment gateway” or “payment switch”. The bank to which the merchant is connected is known as Acquiring Bank or Acquirer.

After the buyer clicks the Check-out button, a new window will be presented on the monitor of the buyer where he inserts his debit card or credit card number, PIN/CVV/CVC, date of expiry etc. and clicks the ‘confirm’ button. The PIN stands for Personal Identification Number, CVV stands for Card Verification Value & used by Visa, and CVC stands for Card Verification Code & used by MasterCard.

The Payment Gateway collects the card information and checks the information for correctness. If the information supplied is found correct, the system debits the buyers bank account or credit card account, and credit the merchant’s account. Then the system informs both the parties about the action.

If the card does not belong to the same bank, the payment gateway sends the information to the payment association (network of MasterCard, Visa, Amex, JBC, Dinar, Discover etc) where the card belongs to. The payment association then sends the card information to the Issuing Bank. Issuing Bank is a bank which issues the card to the customer.

Now the issuing bank verifies the card information and if found correct, debit the buyer’s bank account or card account. This is called **authorization** of transaction. The authorization message goes to the acquiring bank which then credits the merchant’s account (normally offline) and informs both the parties about the action.

The way by which the acquiring bank gets money from the issuing bank, if these are different, is called settlement. The settlement is made daily by the payment associations by debiting the nostro account of issuing bank and crediting the nostro account of the acquiring bank. In case of inland transactions which are routed through NPSB (National Payment Switch, Bangladesh), nostro accounts are accounts of the respective banks maintained with Bangladesh Bank (Central Bank) and incase of transactions made using network of payment association, the nostro account is an account maintained by a local bank with a foreign bank.

Depending on the information obtained from the acquiring bank regarding the action taken, the merchant delivers the goods and services to the buyers address.

Using a payment gateway, cardholder can also pay utility bills such as electricity, gas, water, telephone bills, tuition fees, income tax, city corporation tax, and can buy ticket for train, airplane, bus, steamer, cinema, drama etc. However all such companies should have a website capable to display unpaid bills/fees/tax to the customers after entering the reference number (such as meter number, account number, telephone number etc) by the customer in the company's website. The customer should also be able to pay the unpaid bills by a click on the "Pay" button. In case of buying tickets, the customers may be allowed to view the available seats and select his desired seats from a layout.

5.2. m-Commerce:

M-commerce (or mobile commerce) is the buying and selling of goods and services through wireless handheld devices such as cellular telephone and personal digital assistants (PDAs). M-Commerce is one of the many activities offered by a mobile banking system. The emerging technology behind m-commerce, which is based on the Wireless Application Protocol (WAP), has made far greater strides in almost all the nations. Now-a-day there is no difference between e-commerce and m-commerce as all the buyers can buy all the products and services equally using computer and mobile.

6. Computer Hardware:

Computer is an electronic device which quickly and accurately processes the data and information supplied by human using logic and formula given by human to output result for human being. Human beings undertake decision based on this output.

6.1. History of Development of Computer

Computer is the result of research of hundreds of years. Development of computer starts with the invention of counting machine by various mathematicians like John Napier (1550 – 1617), Blasé Pascal (1642) and Leibniz (1671). Charles Babbage (1792 – 1871), a mathematician of England, developed Difference Engine in 1821. In 1833, he started developing another counting machine in the name of "Analytical Engine", but could not complete before his death. Design of his Analytical Engine is the basis of modern Computer. This is why Charles Babbage is terms as the "**Father of Computer**".

Professor D. John Atanasoff of United States developed an electronic Computer named ABC using vacuum tube in 1942. Later on in 1946, Professor Dr. John Mauchly and his student Engineer Presper jointly developed a computer named ENIAC (Electronic Numeric Integrator And Calculator) on which there were 1800 valves. Its weight was 30 tons, and an electric load of 150 KW was required to run it. These two scientists developed another computer in the name of UNIVAC (Universal Automatic Calculator) in 1951 which had Input, Output and Memory units. This was the first electronic computer produced commercially.

In 1954, the IBM (International Business Machine) company of United States produced a Computer in the name of IMB-701 and starts business.

Bangladesh Atomic Energy Commission installed first computer in Dhaka in 1964. It was an IBM-1620 mainframe computer. Thereafter Bangladesh University of Engineering & Technology (BUET), Bangladesh Bureau of Statistics, Power Development Board installed mainframe computer for their uses.

In 1971, the Intel Company of United States developed MSC-4 microprocessor and introduced Microcomputer.

Due to its development and commercial availability, we can see the use of Microcomputers in educational institutions, business organizations, offices and houses.

6.2. Generations of Computer

Computer can be divided into following four generations:

1st Generation (1951 – 1958):

Characteristics: Use of Vacuum Tube or Vacuum Valve, Big in size, Capability to store program and information, Use of Magnetic Drum, Punch Card and Magnetic tape. Example: ENIAC, MARK, IBM-650.

2nd Generation (1958 – 1965):

Characteristics: Use of IC (Integrated Circuit), Use of transistor instead of Vacuum Tube, Small in size, introduction of ACCII code, development of high-level language like COBOL, FORTRAN and ALGOL. Example: IBM-1620, CDC-1604, NCR-300.

3rd Generation (1965 – 1971):

Characteristics: Introduction of Mouse as input device, Small in size, reduction of price, Introduction of VDO unit and Printer as output device, use of secondary memory, invention of BASIC language, word processing and other applications. Example: IBM-370, PDP-II.

4th Generation (1971 – to date):

Characteristics: Invention and use of Microprocessor, Semi-Conductor memory, ROM, RAM, PROM, EPROM, Higher capacity of storing information, Development of operating systems like DOS, MAC, Windows and Unix, development of various application software and programming languages, development of Super Computer, Laptop, Notebook, Desktop and Personal

Computers. Example: PC, Sever and Laptop of various brands such as IBM, Compaq, HP, Sun, Dell, ACER.

6.3. Types of Computer

Based on the nature of jobs, the Computer can be divided into following three types:

1. Analog Computer
2. Digital Computer
3. Hybrid Computer

Analog Computer is used for special purposes such as measuring pressure and temperature, supply of petrol in petrol pumps and determining price, and controlling speed of a vehicle or Airplane.

Digital Computer works in line with the principles of mathematics. It works using binary systems, i.e., using 1 and 0. The Computers we use at home and office are all Digital computers.

Hybrid Computer collects data from various systems using analog process, but processes the data in digital system.

Figure: A Super Computer

Figure: A Mainframe Computer

Based on size and capacity, Computers (or Digital Computers) can be divided into four types as under:

1. Super Computer
2. Mainframe Computer
3. Mini Computer
4. Micro Computer

Super Computer is very powerful. It requires less time to complete mathematical processes. Super computer is used in scientific research, for processing of large volume of data, for controlling missile, space research, design of nuclear plant. CRAY-1, Super SxII, CYBER-205 are the example of Super Computers.

Mainframe Computer is very large in size. Connecting many small computers into it, many people can work together in a Mainframe Computer. It is used in large organizations like Banks, Insurance Companies and Universities. IBM4300, UNIVAC 1100, NCR 8370 are the example of Mainframe Computers.

Mini Computers are smaller and less costly than Mainframe Computers. Many people can also work in a Mini Computer together using terminals connected to it. Relatively smaller Banks, Insurance Companies, Industries, Educational Institutions and Research Organizations use Mini Computers. IBM S/34 and NCR S/9290 are the example of Mini Computers.

Microcomputers are very small, cheap and widely used computer. As microprocessor is used in this type of computers, they are termed as Microcomputer. Only one person can work at a time in a Microcomputer. For this they are also known as Personal Computer or PC. Microcomputers are used at home and office for personal and official purposes. They are also used for entertainment purposes like playing games, viewing video, listening songs, and browsing internet. IBM PC, Apple PC and Macintosh PC are the example of Microcomputers.

6.4. Computer Hardware and Devices

The devices of a computer may be divided into five parts, like:

Input devices
Output devices
Processing devices
Memory devices
Special devices

6.4.1. Input devices

The devices or parts of the computer used for inputting information, data and instruction into the computer are known as Input Devices. Keyboard, Mouse, Joystick, Scanner, Digital Camera, Microphone etc are the example of input devices.

Figure: A Keyboard

Figure: A Mouse

Keyboard: A Keyboard is a device that contains 104 to 110 number of keys. These keys are used for typing letters and digits and providing instructions to the computer. A keyboard is connected to the motherboard of a computer using a cable.

Mouse: A Mouse is a device used as alternative or associated equipment for providing instruction to the computer having windows or Macintosh operating system in it. The mouse has 2 or 3 buttons.

6.4.2. Output devices

The devices which are used for communicating result to the users are called Output Devices. Monitor, Printer, Speaker and Plotter are the example of output devices.

Monitor: The result of processing activities on certain supplied information and data is displayed using text, graph or picture on a TV like device called Monitor. The Monitor is connected to the system board of a computer using a data cable. In some monitors, a separate power connection is required.

Figure: Speakers

Figure: A Monitor

Figure: A Printer

Printer: The output of a computer is printed on paper using a device called Printer. Printer is connected to the computer's system board using a data cable. Power is supplied to the printer using another cable.

Printer is of two types – Dot Matrix Printer and Laser Printer. Dot matrix printer has a "Head" which creates impact on a ribbon. The ink on the ribbon produces letter, special character and digit on the paper. Epson dot matrix printer, Epson line printer are the example of dot matrix printer. In the Laser Printer instead of Head, laser ray is used to produce letter, special character and digits. Ina Laser Printer, instead of ribbon, a Tonner or Cartridge is used for supplying ink. Ink Jet Printer and Canon Laser Printer are the example of Laser Printer.

Speaker: Speaker is used for creation of sound during listening songs or viewing video.

Plotter: A Plotter is used for printing a drawing from computer. Plotter is also used for printing large picture, poster, calendar and map.

6.4.3. Processing Devices

The devices used for processing of supplied information, data and instructions in a computer are called Processing Devices. CPU or Central Processing Unit is a processing device used in computer. It performs all the processing activities of a computer. CUP is like the brain of human being. The speed and capacity of processing of a computer depends on its CPU.

In 1971, the Intel Company invented microprocessor for use in computer. It was called as 8008 microprocessor. Thereafter Apple produced microprocessor in 1976 and IBM in 1981.

The functionalities of a CPU are stated below:

1. CPU sends controlling and time determining signals to all parts of the computer.
2. Send and receive data between memory and input/output devices.
3. Receive data and instructions from memory.
4. Decode the instructions.
5. Perform mathematical and logical activities.
6. Run program from computer memory.
7. Coordinate between input and output devices.

Based on the architecture, a microprocessor can be divided into 2 groups like CISC processor and RISC processor.

CISC or Complex Instruction Set Computer is a microprocessor which uses microcode. Microcode consists of some instructions (software program) which work from inside the chip. As this type of microprocessor run by software, they are normally slow. Examples of CISC microprocessor are: 8085, 8086, 8088, 80286, 80386SX, 80386DX, 80486SX, 80486DX and Pentium of Intel, 386DX, 486DX of AMD, 6800, 68000, 68040 of Motorola.

RISC or Reduced Instruction Set Computer is a microprocessor in which less number of instructions sets are used. It is not software based, rather hardware based and as such faster than the CISC processor. Banks normally uses RISC processor-based computers as its main database server in the data center. Unix is normally used as operating system of such RISC servers. For example, AIX is used as operating system for IBM RISC servers, Sun Solaris for SUN RISC servers and HP-UX for HP RISC servers.

6.4.4. Memory Device

Memory devices are the devices where the computer temporarily or permanently stores the data before, during and after processing. The memory devices can be categorized into 3 groups: Primary or Main memory, Cache memory and Secondary or Auxiliary memory.

6.4.4.1. Primary or Main memory

The memory directly connected to the CPU is called Primary or Main Memory. It is used to store program, data, instructions and result during execution. RAM and ROM are the example of such memory.

Figure: A RAM

RAM: RAM stands for Random Access Memory. Computer read all the relevant data, program and instructions from the input devices or permanent storage and writes into the RAM for processing. RAM has the following characteristics:

1. RAM is volatile in nature
2. It is a read-write memory
3. During processing the information stay in RAM
4. If power fails, all the information removes from the RAM.

ROM: ROM stands for Read Only Memory. ROM stores a program called BIOS (Basic Input Output System). List, position and specification of all the devices of a computer are recorded into the BIOS. Computer at the time of startup recognizes all the devices with the help of BIOS. The characteristics of a ROM are as under:

1. ROM is a permanent main memory.
2. The information in the ROM can only be read, can't be modified.
3. The programs required to startup a computer are stored permanently in the ROM
4. If power fails, the information at ROM does not vanish.

6.4.4.2. Secondary or Auxiliary memory

The memory which is used to store the user program and information permanently is called Secondary or Auxiliary memory. Examples are: Floppy Disk, Hard Disk, Compact Disk, Magnetic Tape, Pen Drive etc.

Floppy Disk: A light and small disk which is produced by putting a magnetic layer on a thin plastic sheet is called Floppy Disk. The information and program are stored in Floppy Disk. Normally floppy disk is used to transfer information from one computer to another. Floppy disks are of two sizes – 3.5" and 5.25". The device used to read and write information from/to floppy disk is called Floppy Drive. Floppy Drives are also available in two sizes – 3.5" and 5.25".

The capacity of the 3.5" floppy disk is 1.44 MB and that of 5.25" floppy drive is 360 KB.

Due to invention of Pen Drive, the use of Floppy Drive has become unpopular.

Hard Disk: A hard disk is connected inside the computer box using screw and data & power cables, and has much higher capacity and speed than the floppy disk. The data and programs are normally kept stored into the hard disk. No drive is required in the computer for use of hard disk. Hard disk of various capacity is available in the market like 250 GB hard disk, 500 GB hard disk etc.

Compact Disk: Compact Disk is called CD in short. CD is used for recording or storing data, program, song, game, video etc. and also for transferring data from one computer to another. Some CD only allows reading Information from it. The information in it can't be modified. Also new information can't be added into these CD. These CDs are called CD-ROM (Read Only Memory). The drive connected to the Computer and used to read information from CD is called CD Drive. There are some CDs which allow reading, modifying and adding information. These CDs are called Re-Writable CD (CD-RW). For reading, modifying and adding information into a CD-RW, a device is connected with the computer which is called CD Writer. A CD is like a circular disk having a diameter of 4.75". A CD has a capacity of 650 MB.

Figure: A Compact Disk

Figure: A Pen Drive

Magnetic Tape: Magnetic Tape is a plastic reel covered with iron oxide and wrapped in a cassette. Magnetic Tape is used for backing up useful data from hard disk to the tape. This ensures that the data will be available in case of damage of the hard disk. Making duplication of data from hard disk into a magnetic tape is called Backup. Bank daily creates a makeup copy of customer data. A device is connected with the computer using a data cable and used to copy data from computer hard disk to tape drive. This device is called as Tape Drive.

Pen Drive: A Pen Drive is a data storage device which is physically much smaller than a floppy disk but can store mush higher capacity of data like 2GB, 4GB, 8GB and up to 256 GB. They are more durable and reliable because of their lack of moving parts. A Pen Drive is also called as USB flash drive because it is equipped with a USB (Universal Serial Bus) connector at one end. The connector is inserted into the USB port on a computer and the files or data can be copied from/to the pen drive.

6.4.4.3. Cache memory

A special memory placed with the CPU or main memory to increase speed of processing is called Cache Memory. Cache Memory can be classified into two types – Internal Cache and External Cache. Internal Cache is placed inside the microprocessor whereas the external cache is placed on the mother board as IC (Integrated Circuit).

6.4.5. Special Devices

Special devices are devices used to interconnect input, output and memory devices. System Box, Mother Board, Power Supply Unit are the example of special devices.

Figure: A System Box

Figure: A Mother Board and a Power Supply Unit

System Box: A box where the mother board, hard disk, floppy disk, CD drive and power supply unit are connected using screw and cable, is called System Box. Many people wrongly call the

system box as CPU. A system box connected with all the required devices, a monitor, a keyboard and a mouse constitute a computer.

Mother Board: A device which is connected to the system box using screw and which has various slots over which the CPU (processor), ROM and RAM are connected directly, is called Mother Board. The Mother Board has also various ports to which the keyboard, mouse, monitor, floppy drive, CD drive and printer are connected using cable. There are thousands of wires placed inside the mother board which connects various devices internally and carry data and signal from one device to another device. These wire system is called Bus System.

Power Supply Unit: A Power Supply Unit is the component that supplies power to the other components in a computer. More specifically, a power supply unit is typically designed to convert Alternating Current (AC) to Direct Current (DC) which is required for the various components of the computer.

UPS: UPS stands for Uninterrupted Power Supply. UPS is an electrical apparatus that provides emergency power to a computer when the input power source fails, thus protect Computer from sudden shutdown. The UPS can be of two types – Online UPS and Offline UPS. Online UPS has zero transfer time and used with servers, while the offline UPS has a transfer time of 5-10 ms. Both the types of UPS can protect the computer from shutting down in case of power failure, but the online UPS, in addition, can protect data from being garbage/damaged due to power fluctuations as this type of UPS require no transfer time for switching between main power to batter power.

Voltage Stabilizer: A Voltage Stabilizer is an electric regulator designed to automatically maintain an output of constant voltage level irrespective of variation in input voltage. The Voltage Stabilizers are used with Computer System to protect the computer from sudden fluctuation of voltage.

7. Computer Software:

Computer is a machine which can't work itself. To start and make the computer operative, a computer program is required. After the computer is made operative, another set of specific programs are required to perform a specific task. Such programs are collectively known as computer software. Computer software can be divided into two types – System Software and Application Software.

7.1. System Software

The Software used to start the computer and make the computer operational is called System Software. On the other hand, when the Application Software instructs a device of the computer system to do something, the System Software first translates the instruction into a language which is understandable to the device. The System Software then sends the translated

instructions to the respective devices. The devices act accordingly. As such the System Software is positioned in between the computer hardware and the Application Software. The **Operating Systems** are popular System Software.

The Operating System was first developed for the Mainframe Computer in 1960s. Later on various operating systems like Macintosh, Disk Operating System (DOS), Unix and Windows were developed. The Microsoft Company of USA is the developer of DOS and Windows operating systems. The functionalities of an Operating System are as mentioned below:

1. To make the computer active and usable
2. To communicate between hardware and application software
3. To accept and execute the instruction of a user
4. To fetch a program into the main memory and process it
5. To control the activities like writing, storing and reading data to/from Disk.

7.2. Application Software

A program used to perform a specific job using a computer is called Application Software. For example, Word Star, Word Perfect and MS Word are used for typing or word processing; Lotus 1-2-3, Quattro Pro, MS Excel are used for calculation or spread sheet analysis; Netscape Navigator, Internet Explorer, Google Chrome and Firefox are used for web browsing; Out Look, Messenger and Eudora are used for e-mail checking, Power Point is used for presentation; Auto CAD is used for Engineering drawing; SPSS is used for statistical analysis; Access, SQL Server and Oracle are used for data manipulation and storage. These software are developed by different company to sale commercially in the market. The users buy them and use at home and office. For this reason, they are called General Purpose Application Software.

Programmers also develop application software for a specific activity of a specific organization. These are called Application Specific program. For example, a group of programmer or a company may develop a program for a bank for recording transactions of its customers, and at the day-end, to prepare reports like Balance Sheet and Income Statement. The program written for a Bank may not fit to the requirement of another bank, as the transaction rules may be different for different banks.

7.3. Programming Language

The program which is used for writing a General Purpose Program or an Application Specific Program is called Programming Language. Large companies develop Programming Language to sale commercially. Programmers buy these Programming Languages and use one or more of them to write a general-purpose or application-specific program. The commonly used programming languages are:

- C / C++

- Java
- Assembly language
- COBOL
- FORTRAN
- BASIC / BASICA / Q-Basic / Quick Basic
- Visual Basic
- .Net
- HTML
- FoxPro / FoxBase / dBase

The programming languages can be divided into three types:

- Low-Level Languages
- High-Level Languages
- Object Oriented Languages

7.3.1. Low-Level Language

Low-Level languages are languages where the computer programs are written using machine code (binary or hexadecimal codes) or mnemonic code. Low-level language consists of two computer languages – Machine Language and Assembly Language.

Machine Language: During the initial stage of development of Computers, programmers had used machine code, i.e. binary and hexadecimal codes for writing computer program. These computer programs which use machine code from writing a specific user programs are called Machine Language. Machine language can execute very fast and efficiently. However if a specific user program is written using a machine language for a particular computer it can't be run on another computer. Writing, reading and modifying such a computer program is very complex and time consuming. To solve this problem, Assembly Language was developed for writing computer program much comfortably.

Assembly Language: In Assembly Language, instead of machine code such as binary and hexadecimal codes, mnemonic codes are used. For example, assembly language programs use SUB to perform a subtraction operation. For this, assembly language is also called Symbolic language. For developing an operating system, a game or a high-level language, normally the assembly language is used.

7.3.2. High Level Language

A high-level language (developed using assembly language) is very user friendly. It's syntaxes are very similar to English language. A high-level language is used by computer programmers to

develop an application specific computer program. The following are the example of high=level languages:

- COBOL (Common Business Oriented Language)
- BASIC (Beginners All-purpose Symbolic Instruction Code)
- FORTRAN (FORmula TRANslator)
- C
- PASCAL

7.3.3. Object Oriented Language

Object Oriented Language is language that supports the idea of bundling instructions and data into a set of programming code - called an **object.** The object can be used repeatedly throughout the program. The technique of writing a computer program using an object oriented language is called Object Oriented Programming or OOP. An OOP has the following three characteristics:

a. Polymorphism

Polymorphism means different objects respond distinctively to the same message. For example, when we send the same message – "Speak" to a cat object, a dog object, and a cow object, each of one respond appropriately. The cat purrs, the dog barks, and the cow moos.

b. Inheritance

Inheritance means that the language gives us the ability to extend or enhance existing objects. The child object created from the parent object will get all the properties of the parent object and also it can have its own properties.

c. Encapsulation

Encapsulation means that the data and instructions for variables are wrapped up together and treated as a unit. The blueprints for these variables are called **classes** and the units are called **objects**.

The example of object oriented language is C++ and Java.

7.4. Database Management System

Programming language is used to write a computer program for a specific purpose. In such a computer program, there may have some input screens through which the users input data into

the computer system. These data are stored into the computer system for further use or generation of reports later on. For storing data into the computer system in easy retrievable manner, Database is used. A database is a computer program used to store and manipulate data. In a database, the data is kept at row and column as under:

Column / Row	1 (Account No)	2 (Name of Customer)	3 (Account Balance)
1	S101	Ornab Alinur	5000.00
2	S102	Abrar Rahman	3010.00
3	C101	Aminul Islam	2505.00
4	C102	Raiyan Islam	4017.00

In the above example, the file where these information will be stored is called database table. One or more database table together creates a Database. The database and all of its tables have different name. All the tables have rows and columns. In the above example, there are 4 rows and 3 columns.

There are some specific commands for a database to create/modify/delete table, add rows into the table, and ready/modify/delete rows from the table. These commends are called Data Description Language (DDL) and Data Manipulation Language (DML).

Database Management System (DBMS) is a system which not only stores data, but also provides Data Description Language (DDL) and Data Manipulation Language (DML) for the users to create facilities for storing data and manipulation of the stored data.

According to Graham Taylor, the DBMS is a general set of programs designed to link with the application programs of the various users and departments, and the database itself. It controls access (who can use it) and includes facilities for data independences, integrity and security.

DBMS is very useful for a bank. The balance and transactions are recorded into the DBMS. Oracle, DB2 and SQL server are three widely used DBMS in banks.

The officer who is engaged for planning, organizing and controlling a DBMS is called Database Administrator (**DBA**). A DBA is responsible for security and availability of data in the DBMS. If the database is crashed for any reason, it is the responsibility of the DBA to make the data available within shortest possible time. For this reason, the DBA always (normally at the day-end) keeps a copy of the database into a Tape Cartridge and another computer system. This is called taking **Backup** of the database.

8. Internet and related terminologies:

8.1. Internet

The **Internet** is a global system of interconnected computer networks that use the standard Internet Protocol Suite (TCP/IP) to serve billions of users worldwide. It is a *network of networks* that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic and optical networking technologies. The Internet carries a vast range of information resources and services, such as the inter-linked hypertext documents of the World Wide Web (WWW) and the infrastructure to support electronic mail.

Most traditional communications media including telephone, music, film, and television are being reshaped or redefined by the Internet. Newspaper, book and other print publishing are having to adapt to Web sites and blogging. The Internet has enabled or accelerated new forms of human interactions through instant messaging, Internet forums, and social networking. Online shopping has boomed both for major retail outlets and small traders. Business-to-business and financial services on the Internet affect supply chains across entire industries.

The origins of the Internet reach back to the 1960s with both private and United States military research into robust, fault-tolerant, and distributed computer networks. The funding of a new U.S. backbone by the National Science Foundation, as well as private funding for other commercial backbones, led to worldwide participation in the development of new networking technologies, and the merger of many networks. The commercialization of what was by then an international network in the mid 1990s resulted in its popularization and incorporation into virtually every aspect of modern human life. Now, an estimated half of Earth's population is using the services of the Internet.

The Internet has no centralized governance in either technological implementation or policies for access and usage; each constituent network sets its own standards. Only the overreaching definitions of the two principal name spaces in the Internet, the Internet Protocol (IP) address space and the Domain Name System (DNS), are directed by a maintainer organization, the Internet Corporation for Assigned Names and Numbers (ICANN). The technical underpinning and standardization of the core protocols (IPv4 and IPv6) is an activity of the Internet Engineering Task Force (IETF), a non-profit organization of loosely affiliated international participants that anyone may associate with by contributing technical expertise.

8.2. WWW

The World Wide Web, abbreviated as **WWW** and commonly known as **the Web**, is a system of interlinked hypertext documents accessed via the Internet. With a web browser, one can view web pages that may contain text, images, videos, and other multimedia and navigate between them by using hyperlinks. Using concepts from earlier hypertext systems, English engineer and computer scientist Sir Tim Berners-Lee, now the Director of the World Wide Web Consortium,

wrote a proposal in March 1989 for what would eventually become the World Wide Web. The World-Wide Web (W3) was developed to be a pool of human knowledge, and human culture, which would allow collaborators in remote sites to share their ideas and all aspects of a common project.

8.3. Hypertext

Hypertext is text displayed on a computer or other electronic device with references (**hyperlinks**) to other text that the reader can immediately access, usually by a mouse click or keypress sequence. Apart from running text, hypertext may contain tables, images and other presentational devices. Hypertext is the underlying concept defining the structure of the World Wide Web, making it an easy-to-use and flexible format to share information over the Internet.

8.4. Hyperlinks

Hyperlink is a reference to a document that the reader can directly follow, or that is followed automatically. The reference points to a whole document or to a specific element within a document. A user following hyperlinks is said to *navigate* or ***browse*** the hypertext.

8.5. Web browser

A web browser or **Internet browser** is a software application for retrieving, presenting, and traversing information resources on the World Wide Web. Although browsers are primarily intended to access the World Wide Web, they can also be used to access information provided by Web servers in private networks or files in file systems.

8.6. Web Page

A web page or webpage is a document or resource of information that is suitable for the World Wide Web and can be accessed through a web browser and displayed on a monitor or mobile device. This information is usually in HTML or XHTML format, and may provide navigation to other webpages via hypertext links. Webpages may be retrieved from a local computer or from a remote web server. The web server may restrict access only to a private network, e.g. a corporate intranet, or it may publish pages on the World Wide Web.

Webpages may consist of files of static text and other content stored within the web server's file system (**static webpages**), or may be constructed by server-side software when they are requested (**dynamic webpages**).

8.7. Internet vs WWW

The terms *Internet* and *World Wide Web* are often used in everyday speech without much distinction. However, the Internet and the World Wide Web are not one and the same. The Internet is a global data communications system. It is a hardware and software infrastructure

that provides connectivity between computers. In contrast, the Web is one of the services communicated via the Internet. It is a collection of interconnected documents and other resources, linked by hyperlinks and URLs.

8.8. URL

Uniform Resource Locator (**URL**) is a Uniform Resource Identifier (URI) that specifies where an identified resource is available and the mechanism for retrieving it. The best-known example of a URL is the "address" of a web page on the World Wide Web, e.g. http://www.dbbl.com.bd.

8.9. E-mail

Electronic mail, commonly called **email** or **e-mail**, is a method of exchanging digital messages across the Internet or other computer networks. Originally, email was transmitted directly from one user to another computer. This required both computers to be online at the same time. Today's email systems are based on a store-and-forward model. Email servers accept, forward, deliver and store messages. Users no longer need be online simultaneously and need only connect briefly, typically to an email server, for as long as it takes to send or receive messages.

An email message consists of two components, the message *header*, and the message *body*, which is the email's content. The message header contains control information, including, minimally, an originator's email address, one or more recipient addresses and a subject header field. Email can also carry multi-media content attachments.

Review Questions

1. Multiple Choice Questions (MCQ)

i) Which computer was made of Vacuum tube?
a) IBM b) ENIAC c) NCR d) ABC

ii) Which computer was made of Valve?
a) IBM b) ENIAC c) NCR d) ABC

iii) What was the weight of ENIAC computer?
a) 3 tons b) 30 tons c) 3 kg d) 30 kg

iv) The first computer in Bangladesh

- was installed in which year of
a) 1971 b) 1961 c) 1964 d) 1984

- was installed by
a) BUET b) Bangladesh Atomic Energy Commission
c) Bureau of Statistics d) Agrani Bank

- was a type of the computer
a) Super Computer b) Mainframe c) Micro Computer d) PC

v) Which of the following is not an application software?
a) MS Word b) Excel c) Windows d) Firefox

vi) Banking software is a/an
a) Operating System b) Database
c) Application software d) Programming language.

vii) Which one is an Object Oriented Program Language?
a) Java b) Basic c) Fortran d) Cobol

viii) Internet uses a standard internet protocol suite called
a) www b) TCP/IP c) WAN d) Fiber Optic

ix) Which one is not an electronic banking system:
a) ATM b) Internet Banking c) POS terminal d) Cash Counter

x) Which functionality is not available in an Internet Banking System?
a) Cash withdrawal b) Balance Check c) Fud transfer d) Pay Utility Bills

xi) Which of the following is not an input device of a computer?

a) Keyboard b) Scanner c) RAM d) Microphone

xii) Which of the following is not an input device of a computer?

a) Monitor b) Speaker c) Printer d) Scanner

xiii) Which of the following is not a programming language?

a) Java b) C++ c) BASIC d) Excel

2. Fill in the gap:

i) Microcomputer was developed in ------- using ----------.

ii) Operating systems were first developed in ----- for --------.

iii) Internet started in ---- as research work and become International Network in ------.

iv) ATM is used mainly for withdrawal of cash by a bank customer using his debit, credit or ----- card.

v) ATM is supplied with a device for reading a card and a ------ for interaction with the cardholder.

vi) MFS is a banking system for ------- populations.

vii) P2P stands for ----------.

viii) MFS was started in Bangladesh in the year of --------.

ix) Buying and selling of goods and services over ------- is called e-commerce.

x) -------- is called the father of computer?

xi) First electronic computer produced commercially was developed in the year of ------.

xii) Bangladesh Atomic Energy Commission installed first computer in Bangladesh in the year of -------.

xiii) Three types of computer are: -------- computer, digital computer and ------- computer.

ix) Based on the size and capacity, computer can be divided into four types such as -------- computer, -------- computer, -------- computer and micro computer.

x) WWW stands for ---------.

Probable Questions

1. What is the difference between the terms “Information Technology” and “Information and Communication Technology”?

2. Define Information and Communication Technology (ICT).

3. Banking service is now available anytime. How ICT contributed to this?

4. Banking service is now available anywhere. How this become possible after implementation of ICT in Banking?

5. Narrate importance of use of ICT in Banking.

6. Name five electronic banking systems and define them.

7. What are the differences among ATM, CDM and CRM?

8. Name some components of an ATM and mention their functions.

9. How ATMs brings freedom to the customers?

10. Mention five functions of an ATM.

11. What is an ATM booth?

12. What kind of dispute may arise of a CDM? How banks mitigate this?

13. Describe steps of withdrawing money from ATM.

14. Describe various components of a POS terminal.

15. How GPRS POS terminal is different from a dial-up POS terminal?

16. How a bank earns from a POS terminal installed at a merchant?

17. Describe how payment is made using a POS terminal.

18. How Internet Banking works?

19. What banking activities a customer can perform using Internet Banking?

20. Can a customer receive cash from Internet Banking? Why?

21. Mention a few differences between sms and Alert Banking.

22. Mention two syntaxes for any two functions of sms banking.

23. Describe some advantages and disadvantages of Electronic Banking.

24. What is online banking or Any Branch banking? Mention advantages and disadvantages of online banking.

25. What is a MFS? Name a few remarkable MFS in Bangladesh.

26. When MFS started its journey in Bangladesh and which bank stated it?

27. What are the services a MFS operator provides in Bangladesh? Name 5 most used services which approximate amount of transactions through each of the services held in Feb, 2022.

28. As per the MFS policy, how much share a bank shall hold in the MFS?

29. In relation to e-commerce, define the following: Cart, Payment gateway, Acquiring and Issuing Bank, PIN, CVV, CVC, Payment Association, Authorization, Settlement, Nostro account, NPSB.

30. Describe process flow of payment in ecommerce.

31. Describe settlement process for ecommerce trasactions.

32. What is a computer? Who is the father of computer?

33. Describe different generation of computers.

34. Different types of computer are Analog, Digital and Hybrid. Describe each of them.

35. Based on size & capacity, computer can be divided into Super, Mainframe, Mini and Micro computers. What are the differences among them?

36. Why micro computers are also called as PC?

37. Name five input devices and 3 output devices. Describe printer, keyboard and mouse.

38. Differentiate between a dot matrix and a laser printer.

39. What stand for CPU? What is its use in computer?

40. What are CISC and RISC processor? Which processor is used in a high-end IBM server?

41. Narrate characteristics of each of the Main, Cache and Secondary memory.

42. What are differences among Floppy disk, Hard disk, CD and Pen drive?

43. What is a mother board?

44. Why an UPS is used with a computer?

45. What are the differences between a system software and application software?

46. What are the functionalities of an operating system?

47. Why a database is used along with a program?

48. Describe the following: a) DBA, b) Backup c) Database Management System

49. Define the followings: a) Internet, b) IP, c) DNS, d) Hyperlink, e) URL, f) email

50. Identify differences between IPv4 and IPv6?

51. What is World Wide Web? What is the basic difference between www and Internet?

Module-B

Different Approaches to Automation of Financial Institutions (FIs)

1. Data Center (DC), Near DC, Disaster Recovery Site (DRS), Data Center Standards and Certifications

1.1. Data Center (DC)

Figure: A Data Center

A **data center** is a facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and security devices.

There are 4 types of data center. The simplest is a Tier 1 data center, which is basically a server room, following basic guidelines for the installation of computer systems. The most stringent level is a Tier 4 data center, which is designed to host mission critical computer systems, with fully redundant subsystems and compartmentalized security zones controlled by biometric access controls methods. Each of the 4 levels of DC are narrated below:

Tier Level	Requirements
1	• Single non-redundant distribution path serving the IT equipments • Non-redundant capacity components • Basic site infrastructure guaranteeing 99.671% availability
2	• Fulfils all Tier 1 requirements • Redundant site infrastructure capacity components guaranteeing 99.741% availability
3	• Fulfils all Tier 1 & Tier 2 requirements • Multiple independent distribution paths serving the IT equipments • All IT equipments must be dual-powered and fully compatible with the topology of a site's architecture • Concurrently maintainable site infrastructure guaranteeing 99.982% availability
4	• Fulfils all Tier 1, Tier 2 and Tier 3 requirements • All cooling equipment is independently dual-powered, including chillers and

	Heating, Ventilating and Air Conditioning (HVAC) systems • Fault tolerant site infrastructure with electrical power storage and distribution facilities guaranteeing 99.995% availability

A data center can occupy one room of a building, one or more floors, or an entire building. Most of the equipment is often in the form of servers mounted in rack cabinets, which are usually placed in single rows forming corridors between them. This allows people access to the front and rear of each cabinet. Air Conditioning is used to control the temperature and humidity in the data center. The recommended temperature ranges from 16–24 °C (61–75 °F) and humidity range from 40–55% with a maximum dew point of 15°C as optimal for data center conditions.

1.2. Near DC

Near Data Center is a data center established in the same city where the main data center is located. The main data center and the near data center are sometimes refers as DC1 and DC2. Both the DC1 and DC2 are installed with similar hardware and other devices and software and must be setup in an active-active mode. All the resources of both the data centers are utilized simultaneously at 50-50 load. If one of the DC1 and DC2 goes down for any reason, the other one should be able to run the operation of the bank alone without any interruption and these operation switching activities are made automatically – users in branches, ATMs and other channels will not experience any interruption of service. The DC1 and DC2 should be accessible to the IT people easily at minimum travel time from their IT office. The IT Office is an office other than DC1 and DC2 where the IT experts sit and perform all the IT related activities.

1.3. Disaster Recovery Site (DRS)

Disaster recovery is the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster. **Disaster Recover Site** is a place similar to Data Center in term of infrastructure, hardware and software installed, and data stored. The DRS should have capability to become primary site automatically in case the Data Center is in disaster.

The distance between the Data Center and DRS needs trade-off between the following two issues:

i) If long distance is chosen, there may be problem related to manageability of the DRS, availability of dark fiber and availability of required latency. Also the sync replication may not be possible.

ii) If short distance (at least 20 km) is chosen, the disaster like earthquake, hurricane may destroy both the site.

1.4. Data Center Standards and Certifications

Data center certification and standards ensure operational safety of data center and continuity of operation. This also ensures high reliability and performance which can be hard to achieve in a common company's server room. One of the common data center certifications awarded by the “Uptime Institute” is Tier certification (Tier-1, Tier-2, Tier-3 or Tier-4).

Whereas the data center security standards ensure high level of data center security. The most common security standards are ISO 27000, PCI DSS, HIPAA, TIA 942 or AICPA SOC. Data Center Security Standards will be discussed in Module-D.

Data Center Tiers:

- **Tier-1:** These data centers are best suited to small businesses and start-ups looking for the most affordable hosting option. Small firms without complex IT requirements that can tolerate more frequent downtime is suitable to adopt Tier-1 standard. Tier-1 data center has a single path for power and cooling, and no backup components. This tier has an expected uptime of 99.671% per year.

- **Tier-2:** These facilities are the go-to option for SME businesses that want a cost-effective, more reliable option than a tier-1 standard. Small to medium-sized firms typically use tier 2 facilities, often to host non-mission-critical databases. Tier-2 data center has a single path for power and cooling, and some redundant and backup components. This tier offers an expected uptime of 99.741% per year.

- **Tier-3:** These types of data centers are ideal for large companies with IT operations that need extra fail-safes. Businesses that host extensive data sets (particularly customer data) are prime candidates for this tier. Tier-3 data center has multiple paths for power and cooling, and redundant systems that allow the staff to work on the setup without taking it offline. This tier has an expected uptime of 99.982% per year.

- **Tier-4:** These data centers fit enterprises without budget constraints that require uninterrupted availability. Government organizations, Banks and large enterprises with mission-critical servers and intense customer or business demands are typical users of a tier-4 facility. Tier-4 data center is a completely fault-tolerant data center with redundancy for every component. This tier comes with an expected uptime of 99.995% per year.

Typically, the two primary considerations when choosing a tier are **cost** and **uptime**.

2. Computer Networking

2.1. Concept of LAN and WAN

2.1.1. Local Area Network

A Local Area Network (LAN) is a Computer Network covering a small physical area, like a branch, home, office, or small groups of buildings, such as a school, or an airport. LAN connects more than one computer and is useful for sharing resources like files, printers, games or other applications. A computer connected to a LAN is able to access data and share program in another computer in the same LAN. Users can also use the LAN to communicate with each other, by sending e-mail or engaging in chat sessions.

A LAN Card is installed on each of the computers. The LAN Card has a port where one end of a cable is connected. Another end of the cable is connected to a Hub or Network Switch. Similarly all the computers are connected to the Hub or Network Switch to build the LAN. The run length of individual *Ethernet cables* is limited to roughly 100 meters.

The following characteristics differentiate one LAN from another:

Figure: Network Cables

Topology: The geometric arrangement of devices on the network. For example, devices can be arranged in a ring or in a straight line.

Protocol: The rules and encoding specifications for sending data. The protocols also determine whether the network uses a peer-to-peer or client/server architecture.

Media: Devices can be connected by twisted-pair wire, coaxial cables or fiber optic cables. Some networks do without connecting media altogether, communicating instead via radio waves.

LANs are capable of transmitting data at very fast rates, much faster than data can be transmitted over a telephone line; but the distances are limited, and there is also a limit on the number of computers that can be attached to a single LAN.

The defining characteristics of LANs, in contrast to Wide Area Network (WAN), include their usually higher data-transfer rates, smaller geographic area, and lack of a need for leased telecommunication lines.

2.1.2. Wide Area Network

Wide Area Network (WAN) is a computer network that spans a relatively large geographical area. Typically, a WAN connects two or more local area networks (LAN).

Computers connected to a wide-area network are often connected through public networks, such as the telephone system (X.25 and DDN). They can also be connected through leased lines (Radio, Fiber Optic etc.) or satellites (VSAT). All the computers in a LAN are connected to a **network switch**. The network switch has a connection to a **router** which is the gateway for the LAN. All the routers of different LANs participating in the WAN are then connected together using telephone system, leased lines or satellites. Network protocols like TCP/IP, X.25, ATM, Frame Relay are used to deliver transport and addressing functions – that is, for locating a computer in the WAN and determining route for transferring data/information and/or communication.

For a Bank, each branch has a LAN. All the Computers in the branch are connected to one or more network switch. The network switch is connected to a router. If a bank has 100 branches, it has 100 routers installed in individual branches. Now all the routers are connected together to form a WAN. All the routers are connected using fiber optic leased lines, Radio links or satellites (VSAT). They are collectively known as communication media.

The largest WAN in existence is the **Internet**.

Using WAN, users and computers in one location can communicate with users and computers in other locations. Many WANs are built for one particular organization and are private. Others,

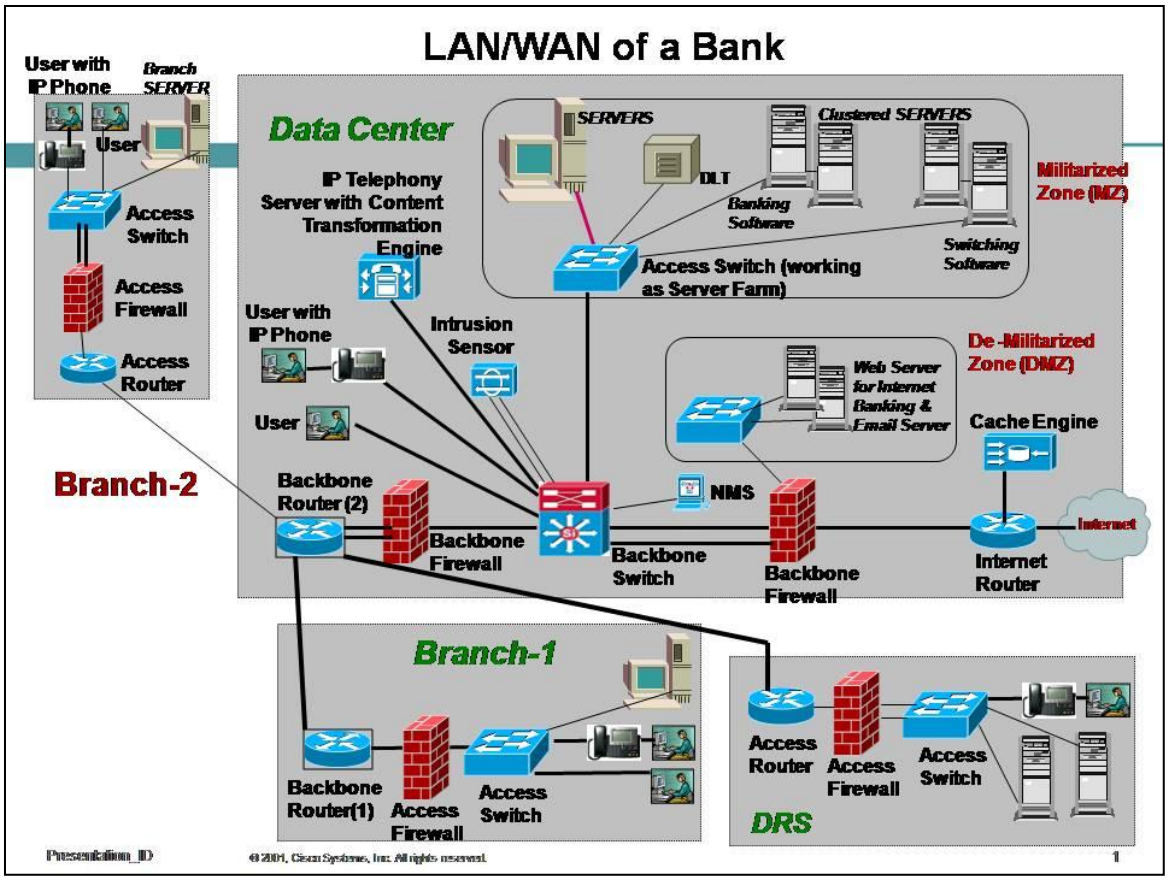
built by Internet Service Providers, provide connections from an organization's LAN to the Internet.

2.1.3. Transmission Media

Transmission or communication media is the physical media used for connection of computers on LAN and WAN.

2.1.3.1. Transmission Media for LAN:

For LAN, there are many different types of transmission media, the most popular being twisted-



pair wire (normal electrical wire), coaxial cable (the type of cable used for cable television), fiber optic cable (cables made out of glass) and wireless media (Wi-Fi).

A Wi-Fi enabled device such as a computer, mobile phone, MP3 player can connect to the internet when within range of a wireless network that is connected to the Internet. The coverage of the wireless network called Wi-Fi hotspots, can comprise an area as small as a few rooms, a hotel, an university or an airport. Wi-Fi hotspots can provide public access to internet either to every one free-of-charge, or to subscribers to various commercial services.

2.1.3.2. Transmission Media for WAN:

For WAN, the transmission media can be land telephone system (X.25, DDN, ISDN), leased land lines (Fiber Optic), Microwave (Radio) or satellites (VSAT).

a) Land Lines:

Land telephone systems use direct copper cabling between two routers. These are slow (less bandwidth up to 2 MB) and not available throughout the country. Fiber Optic has very high bandwidth (service providers can provide up to 10 GB depending on interface card), but only available in large cities.

b) Microwave:

Microwave or Radio link use microwave of public frequencies (2.4, 5.7 & 5.8 Ghz) as well as licensed frequencies (3.2 & 5.2 Ghz). Two points are connected using high towers and antenna. The two antennas connecting two LAN must be at eye-to-eye, i.e., there should not be any obstacle like building or hill in between two antennas. The distance between the two antennas should not be more than 30 km. The bandwidth can be a maximum of 10 MB depending on interface card (i.e., if the speed of the interface card is 10 MB).

Mobile phone system uses wireless technology for data connectivity. These systems provide low bandwidth (speed) and may be used for connecting Automated Teller Machines (ATM) with the bank's data center.

c) Satellites:

Satellites (VSAT – Very Small Aperture Terminal) can cover a long distance. In case of use of VSAT, there is no requirement for eye-to-eye placement for VSAT antenna. However the VSAT provides small bandwidth (up to 1 MB) which may not be sufficient for running banking applications.

2.1.4. LAN/WAN for Bank

For setting up a LAN/WAN, we need Hub/Network Switch and Router. However, for a bank, which deals with money and as such where security is the main concern, additional security devices like **Firewall** are required at Data Center, DRS and each of the branches. The firewall is installed in between Switch and Router. The Firewall guarantee that the instructions entering into the Data Center are from designated branch.

2.1.4.1. Firewall:

A firewall is a part of computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device which is configured to permit or deny computer applications based upon a set of rules and other criteria. Firewalls can be implemented in either hardware or software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet.

2.1.4.2. DMZ:

Special security attention needs to be given during providing internet connection in the Data Center. The servers related to internet access should be placed in the **De-militarized Zone (DMZ)**.

In computer security, a DMZ or demilitarized zone is a physical or logical sub-network that contains and exposes an organization's external services to a larger un-trusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's LAN; an external attacker only has access to equipment in the DMZ, rather than any other part of the network.

3. IT Systems, Storage and Database Backup systems

For Bank automation a huge quantity of hardware, storage and software are required. The Servers, Personal Computers, UPS, various software, networking equipment and other accessories require a big investment. For automation of a bank of 50 branches, the required budget should be around Tk.500 - 1000 million. This budget includes only setup of data center, DRS, installation of facilities for bringing all the branches in online operation with a core banking solution and does not include installation of any delivery channel.

3.1. IT Systems and Storage

IT Systems includes all types of hardware excluding storage systems which are Severs, Personal Computers, Laptops, Printers, UPS, Voltage Stabilizers, Generators etc. Storage systems includes external storage, SAN switch etc. Below is a discussion on various types of Severs, technology related to server installation (RAID, Clustering and Replication) and External Storage & SAN Switch.

3.1.1. Computer Servers and types:

Computer servers are used in branches and Data Centers which manages other computers in a branch or manages a software system or database. Various types of servers are described below:

a) Branch Server:

In a LAN of a branch, all the users' (bank officer's) computers are connected. There may have one or more servers for different purposes connected to the LAN. One such server may be used for accessing Core Banking System of the bank installed centrally at Data Center and called branch server. Branch server facilitates branch users to access the central application servers for executing transactions online real-time basis.

Earlier versions of Core Banking Software were designed to work in 4 steps – at user terminal, branch server, application server, and database server. Branch server was used to perform some activities offline and to validate some functionality locally from the branch server which in turn reduces the bandwidth requirement in WAN connectivity. Offline capability ensures that during break down of the WAN connectivity, the branch users can make offline transactions only for their own (home branch) customers. Such offline transactions are validated from and recorded to the database of the branch server. After the connection is established, all the transactions are sent to the central database server for update. Branch server records signature and photograph of the customers of the home branch and during transaction from the home branch, these are displayed at the user's terminal from the branch server for verification. This reduces the bandwidth requirement. The signature and photograph are also recorded in the central database server at the Data Center. If a customer makes transaction from another branch, these are displayed at the user's computer from the data center.

However, as bandwidth has become available in abundant and become less costly, banks are now using redundant links between Data Center and Branches. As such, such software functionalities are now become unnecessary.

b) Application Server:

When a bank officer (user) makes a posting at his computer terminal, it is partially validated at branch server and then the data and instructions pass through WAN to the Application Server at Data Center. An Application Server is a server which contains main part of the program written for the specific purposes. In the **3-tier architecture** of programming technique, normally user's computer terminal, application server and database server are involved. A part of the program is installed at the user's computer terminal, user has to run this program by clicking an icon or menu. This program automatically gets connected to the Application Server. Application server interacts with the user providing various menu, sub-menu, prompt, window etc. and collect data and instructions. Finally, for execution of the instructions, the data is handed over to the databases server.

c) Database Server:

Database server stores customer data. It also validates some business rules and consistencies before customer data is modified. Database server gets instruction from the Application Server for modifying customer data. It validates some business rules like the account has sufficient balance to withdraw, the cheque leaf is unpaid etc. If the validation is passed, the database server updates the account position and stores the transaction in the history.

3.1.2. RAID

RAID stands for Redundant Array of Independent (or inexpensive) Disks and used in case of internal storage of a server having multiple hard disks or in the external storage systems for increasing data reliability.

RAID is a technology used for hard drives of Computer Servers to provide data reliability and increase input/output performance. When multiple physical disks are set up to use RAID technology, they are said to be *in* a RAID array. This array distributes data across multiple disks, but the array is seen by the computer user and operating system as one single disk.

There are number of different RAID levels:

Level 0 -- Striped Disk Array without Fault Tolerance: Provides *data striping* (spreading out blocks of each file across multiple disk drives) but no redundancy. This improves performance but does not deliver fault tolerance. If one drive fails then all data in the array is lost.

Level 1 -- Mirroring and Duplexing: Provides disk mirroring. Mirroring is a technique in which data is written to two duplicate disks simultaneously. This way if one of the disk drives fails, the system can instantly switch to the other disk without any loss of data or service.

Level 2 -- Error-Correcting Coding: Not a typical implementation and rarely used, Level 2 stripes data at the bit level rather than the block level.

Level 3 -- Bit-Interleaved Parity: Provides byte-level striping with a dedicated parity disk. Level 3, which cannot service simultaneous multiple requests, also is rarely used.

Level 4 -- Dedicated Parity Drive: A commonly used implementation of RAID, Level 4 provides block-level striping (like Level 0) with a parity disk. If a data disk fails, the parity data is used to create a replacement disk. A disadvantage to Level 4 is that the parity disk can create write bottlenecks.

Level 5 -- Block Interleaved Distributed Parity: Provides data striping at the byte level and also stripe error correction information. This results in excellent performance and good fault tolerance. Level 5 is one of the most popular implementations of RAID.

Level 6 -- Independent Data Disks with Double Parity: Provides block-level striping with parity data distributed across all disks.

Level 0+1 -- A Mirror of Stripes: Not one of the original RAID levels, two RAID 0 stripes are created, and a RAID 1 mirror is created over them. Used for both replicating and sharing data among disks.

3.1.3. Clustering

Clustering is grouping of linked computer servers, working together closely so that in many respects they form a single computer server. Based on the purpose of making a cluster between two computers, the clustering can be of the following types:

a) High-availability (HA) clusters

High-availability clusters (also known as Failover Clusters) are implemented primarily for the purpose of improving the availability of services. They operate by having redundant nodes (servers), which are used to provide service when the first node fails. The most common size for an HA cluster is two node, which is the minimum requirement to provide redundancy. HA cluster implementations attempt to use redundancy of cluster components to eliminate single point of failure. This is also called **active-passive cluster**.

b) Load-balancing clusters

In a Load-balancing clusters, two computers are linked together to share computational workload at 50% load and function as a single virtual computer. Requests initiated from the user are managed by, and distributed among all the computers by a network load balancer. This results in balanced computational work load among different machines, improving the performance of the cluster system in one side, and providing redundancy on the other side. If one node fails the other node run at 100% load. This is also called as **active-active cluster**.

3.1.4. Replication

Replication is a set of technologies for copying and distributing data and database objects from one database to another and then synchronizing between databases to maintain consistency. Using replication, data can be copied to a remote location normally from Data Center to DRS using a high speed link. Replication can be asynchronous (async) or synchronous (sync).

a) Async Replication:

In an async replication, data is transferred from DC to DRS after a set time interval say 5 minutes. This type of replication can be made using fiber optic connectivity.

b) Sync Replication:

In a sync replication, data is transferred instantly from DC to DRS meaning as and when a transaction is recorded in DC, it will be recorded simultaneously at DRS also. For sync replication, a dark fiber is required.

3.1.5. Dark Fiber:

A dark fiber is a dedicated direct fiber optic link between two points, normally used for replication of data between DC and DRS. Dark fibers are not shared, and routers are not

connected at two ends of the fiber cable (as such TCP/IP protocol is not used for communication). Their bandwidth very high and speed of transmission of data is very fast.

3.1.6. External Storage System

In a bank, the volume of data is huge which the internal hard disks of a computer server can't accommodate. It requires 50-500 numbers of hard disk to store the customer information and record everyday transactions. In an external storage device, all these hard disks are placed. The device also contains processor, RAM, software etc. to manage the hard disks – normally to allocate the space for different applications running on different servers. As such the external storage system also uses for storage consolidation. Such storage system has capability to replicate data from Data Center to DRS.

3.1.7. SAN Switch:

The storage device is connected to servers through SAN Switch. SAN stands for Storage Area Network, and is a specialized, high-speed network attaching servers and storage devices.

3.2. Database backup systems

Database stores important data related to customer, their transactions and credit card. It is very important to protect these data from loss. Database backup is a way to protect and restore a database. Typically, database backup is performed by the RDBMS or similar database management software. In case of disaster, the Database Administrator (DBA) can use the database backup copy to restore the database to its operational state along with its data and logs. The database backup can be kept locally or on a backup server or on cloud.

Database backup is also created/performed to ensure a company's compliance with business and government regulations and to maintain and ensure access to critical/essential business data in case of a disaster or technical outage.

Types of Database Backup:

a) Full backups

The most basic and complete type of backup operation is a full backup. As the name implies, this type of backup makes a copy of all data to a storage device, such as a disk or tape. The primary advantage to performing a full backup during every operation is that a complete copy

of all data is available with a single set of media. This results in a minimal time to restore data, a metric known as a recovery time objective. However, the disadvantages are that it takes longer to perform a full backup than other types (sometimes by a factor of 10 or more), and it requires more storage space.

Thus, full backups are typically run only periodically. Data centers that have a small amount of data (or critical applications) may choose to run a full backup daily, or even more often in some cases. Typically, backup operations employ a full backup in combination with either incremental or differential backups.

Restore operation is simple and requires less amount of time as only the latest backup can result in the full recovery of data.

b) Incremental backups

An incremental backup operation will result in copying only the data that has changed since the last backup operation of any type. An organization typically uses the modified time stamp on files and compares it to the time stamp of the last backup. Backup applications track and record the date and time that backup operations occur in order to track files modified since these operations.

Because an incremental backup will only copy data since the last backup of any type, an organization may run it as often as desired, with only the most recent changes stored. The benefit of an incremental backup is that it copies a smaller amount of data than a full. Thus, these operations will have a faster backup speed, and require less media to store the backup.

The full backup taken on the first day of the latest backup period and the subsequent incremental backups are required for restore operation. This can dramatically increase recovery times, and requires that each media set work properly; a failure in one backup set can impact the entire restoration.

c) Differential backups

A differential backup operation is similar to an incremental the first time it is performed, in that it will copy all data changed from the previous backup. However, each time it is run afterwards, it will continue to copy all data changed since the previous full backup. Thus, it will store more backed up data than an incremental on subsequent operations, although typically far less than

a full backup. Moreover, differential backups require more space and time to complete than incremental backups, although less than full backups.

The full backup taken on the first day of the latest backup period and the last differential backup are required for restore operation. This reduce the time needed to recover and the potential for problems with an unreadable backup set.

4. FI Computerization approaches

There are various approaches for automation of Banking activities. The initial automation starts with use of stand-alone computer in Banks. Thereafter gradually LAN, WAN with distributed database and WAN with centralized database were introduced in different Banks. Introduction of centralized database facilitate the Banks to start **e-banking**. E-banking covers different electronic banking channels like ATM, POS, Internet Banking, sms and Alert Banking, e-commerce, m-commerce and Call Center. Using these electronic channels, the Banks can offer different banking services to their customers. These electronic channels are also collectively called as **Alternative Delivery Channels**. To use many of the Alternative Delivery Channels the customer needs a plastic card. The plastic card can be a debit card, a credit card or a smart card. These cards are collectively known as **Plastic Money**. For production and management of plastic cards, banks need to install various software and be member of various local and international payment associations like Q-Cash, MasterCard and VISA card.

The following paragraphs narrate the various approaches to Bank Automation. Next chapters will discuss the Plastic Money and Alternative Delivery Channels.

4.1. Stand-alone System

In eighties, Banks in Bangladesh started computerizations just to replace the customer ledger. The software used for replacement of customer ledger, was used by the branch for posting debit and credit entries at the customer accounts during receipt and payment at bank counter. No other banking activities like credit and foreign trade functionalities, and back office activities like calculation of interest, service charges, fees and commissions, maintaining general ledger, preparation of chart of accounts, statement of income-expenses and other reports were not included in the software.

The software was stand-alone, that is, it was not sharable by more than one computer. It should be installed in one computer of a branch. One computer operator was posted for data

entry. The Teller receives the check and passes to the Computer Operator for posting. After the posting was made successfully, the Teller handed over money to the customer. However, the receipt vouchers could be posted after close of the transaction hours.

The big disadvantage of the stand alone system is that it could not be used for the large branch where number of transaction is huge. Another disadvantage is the absence of all banking functionalities in the system.

Beximco Computers was pioneer in developing the first stand-alone banking software in Bangladesh in the name of “BexiBank”.

4.2. LAN-based System

In the nineties, the LAN-based Core Banking Software comes into picture. In a LAN-based system, the software was installed on a Computer Server. The Computer Server was connected to a HUB or Network Switch. All other computers called work stations were connected to the Server through this HUB or Network Switch. Each of the Tellers and Back Office Officers were given a work station for posting. All the customer and account related information and transactions were recorded in the hard disk with the Server.

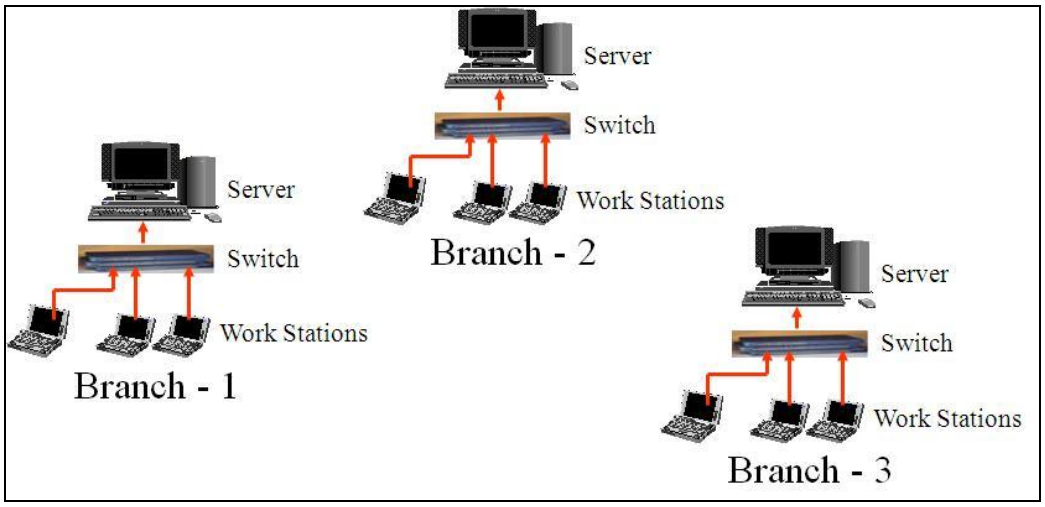


Figure: A LAN-based Core Banking System

For establishing LAN among the computers, Unix or Novel operating system was used. The data was stored in the Server in a flat file or a database – either FoxPro or dBase. The application software was written in COBOL, FoxPro or dBase.

LAN-based core banking software was developed by various companies in Bangladesh, a list of which is given below:

SL	Name of Software	Name of Developer
1	PcBank PcBank/M PcBank2000	Leads Corporation Ltd.
2	BexiBank3000, BexiBank3000+ BexiBank4000 BexiBank5000	Beximco Computers Ltd.
3	A-Z Banking Software	A to Z Computers Ltd.
4	EaseBank	Computer Ease Limited
5	IBS	Infinity Technology International Ltd.
6	E-Banking	Desktop Computer Connection Ltd.
7	Kernel	Kernel Software limited
8	FloraBank	Flora Limited
9	Millennium	Southtech Limited
10	TIBS	Technoheaven Limited

In the LAN-based software, many banking features were included. However, the accountholders data was stored and available in a branch only and thus on-line banking was not possible using such software.

The costing of such software was very low, only Taka 50,000 – 70,000 per branch.

4.3. WAN-based System with distributed database

In 2000, Bangladesh Telephone and Telegram Board (BTTB) installed the DDN (Digital Data Network) switch at its Mogbazar Exchange. DDN is a data communication media using normal telephone line at a maximum speed of 256 Kbps and was available at district towns in Bangladesh. Using this communication media, some banks started establishing WAN among the branches at district towns.

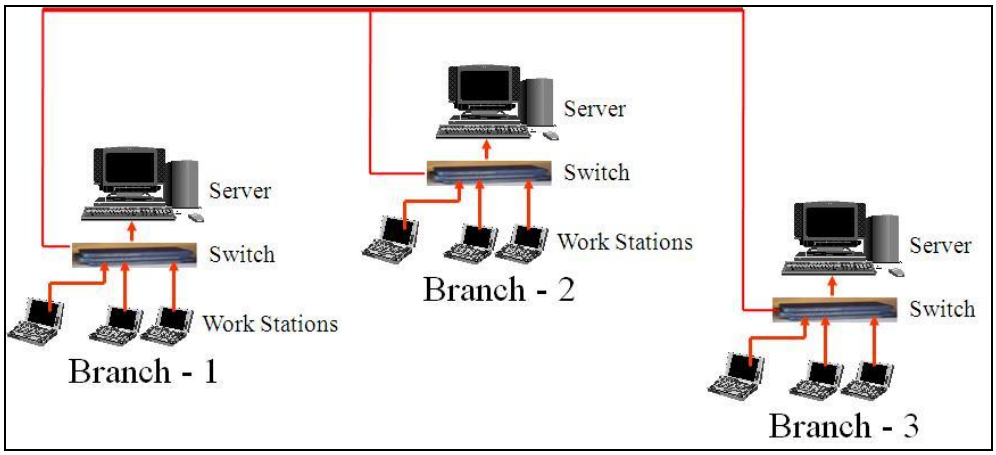


Figure: A WAN-based core banking system with distributed database

The WAN thus established was used to connect different LANs in different branches and thus provided facilities for the customer to go into another branch and withdraw or deposit money. This had started an era of **semi-online banking**. The customer needed to declare the name of branches from where he wanted to get on-line services. The home branch of the customer would make copies of the customer's signature card and photograph, and send to the declared branches for authentication during on-line transactions. The Tellers of other branches entered into the server of the customer's home branch using WAN connectivity and a special password, and made the posting.

The software used for WAN-based transactions was exactly same as one used for LAN-based transactions except a minor customization to accept transaction from other branch.

However, this system was not considered as a complete solution for on-line banking. This system does not support inclusion of various delivery channels like ATM, POS, Internet Banking system, sms & Alert Banking system. Using this system, if a bank wants to include ATMs, it will need to keep all the branches open 24 hours a day and 7 days a week. This is not possible, as the servers are not sized for 24-hours of operation, and many other factors like expert manpower, proper electric power, adequate air conditioning system may not be feasible at all the branches.

True on-line banking can be achieved by installing a centralized core banking system. Among the local banks, the AB Bank, at that time, was using a centralized core banking system named "Equation". However only the branches at Dhaka city were connected to this centralized core banking system.

4.4. WAN-based System with centralized database

In 2004, the centralized core banking system was installed simultaneously by Eastern Bank, Dhaka Bank and Dutch-Bangla Bank. All the three banks procured a core banking software named “Flexcube” from i-flex solutions limited, India. The software was installed centrally at the “Data Center” of the bank. LANs were installed at each of the branches and all the LANs were connected to Data Center using VSAT, Radio Link, DDN or Fiber Optic Cable or a combination of them. Two redundant links were used for connecting each of the branches.

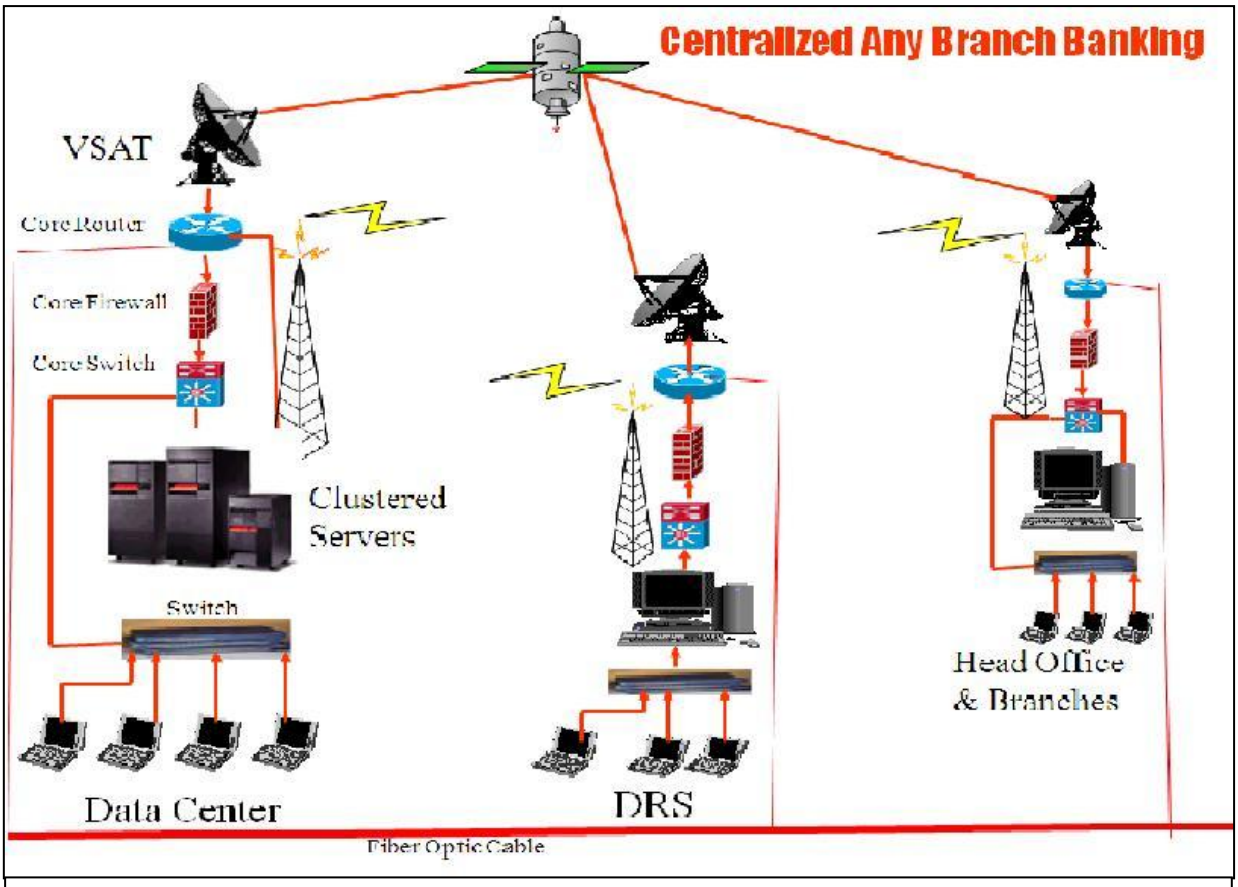


Figure: a WAN-based Core banking System with centralized database

In the centralized core banking system, all the customers’ information and transactions are recorded centrally at a storage system connected with a group of clustered servers at Data Center. Clustered Servers provides redundancy to the system, thus if one server fails, another server takes over the control of the system and serves all the branches. However, in this type of solution, Bank needs to establish Disaster Recovery Site (DRS) in a distant location for maintaining an online copy of the database and also for housing a redundant set of servers and equipment.

In the centralized core banking system, alternative delivery channels like ATM/POS can be integrated easily as the ATM/POS system will be connected to the Central Server, not to the individual branches. And the central servers, equipment and environments are sized to run 24 hours a day, 365 days a year. Expert IT professional can be made available at the Data Center and the roaster duty can be arranged for 24-hour's monitoring of the Data Center.

Thereafter, the 'One Bank' moves to Centralized Core Banking System using "Microbanker" of i-flex solutions ltd, India; BRAC Bank and City Bank using "Finacle" of Infosys Limited, India; Prime Bank and EXIM Bank using T24 of Globas Pvt Ltd. Switzerland; AB Bank and IFIC Bank using Equation of Misys Plc, UK; and BASIC Bank using "Kastle Core Banking" of 3i Infotech Limited, India.

Meantime the local software companies like Flora Systems, Leads Corporation, Millennium Software and ERA Infotech have developed Centralized Core Banking Software in the name of "Flora Bank Online", "Bank Ultimas", "Ababil" and "Stealer" respectively.

Rest of the Banks started using locally developed Centralized Core Banking Software after 2007.

5. Various Software Systems for FIs

In Banks, many software are used for various purposes. The software used for opening bank account by deposit and loan customers, and recording their transactions is called Core Banking Software. For managing ATM and POS network, a Switching Software is needed. For credit card issuance and transaction authorization, Credit Card Software is used. Payment Gateway Software is used for settlement of e-commerce transactions. A Mobile Banking Software may be used for opening mobile account and recording such transactions. A brief description of the major software used by banks is given below.

5.1. Core Banking Software

Core operations of a Bank includes maintaining a ledger of various transactions, keeping customer information, interest calculation of loans and deposits, adjustments to accounts on withdrawal and deposits of funds etc. Previously these operations were done manually. With the advent of ICT (Information & Communications Technology), efforts were done to automate various banking processes using software applications so as to make them simple, efficient, effortless and cost effective. Thus, the platform where ICT is used to perform the core

operations of a bank, like those mentioned above, is known as Core Banking System and the software used for this purpose is called Core Banking Software.

In Core Banking System (CBS), the data, instead of huge ledgers, are stored in backend databases in digital form. The same software can be made available in various branches of a bank using a WAN. The advantage, a customer can operate on his account from any branch of the bank and if the bank owns Internet Banking or ATM facilities, then the customer can operate on his account from virtually anywhere.

CBS has facilitated better operational efficiency by ensuring improved house keeping and preventing seepage of income. Inter branch reconciliation has become faster and accurate.

Thus, Core Banking System has radically changed the way in which banks function. The greatest advantage of having a Core Bank System is that introduction of new facilities and products wouldn't be a time-consuming process, and branch clearings would become instantaneous. Electronic funds transfer between banks, online trading in the stock markets etc. are examples, which were unheard of in banks pre Core Banking System era.

The international Core Banking Applications now-a-day available in the market are T24 of Temenos, Oracle Financial Services Software (OFSS) of Oracle, Finacle of Infosys, Equation of Mysis, TCS BaNCS of Tata Consultancy and Intellect Suite of Polaris.

The Core Banking Software available locally are “Flora Bank Online” of Flora Systems Ltd., “Bank Ultimas” of Leads Corporation, “Ababil” of Millennium Software and “Stealer” of ERA Infotech.

5.2. Switching Software

A Switching Software is an ATM/POS transaction processing and management system which is used for the following specific purposes:

i) Production of **Debit Cards** which, in addition, includes insertion of customer’s data into the system and storing the inserted data into a database,

ii) Pre-authorization of on-us debit card transactions (transactions made by bank’s own cardholders at bank’s own ATM/POS) or remote on-us debit card transactions (transactions made by bank’s own cardholders at ATM/POS of another bank). Note: pre-

authorization includes validation of Card Number, PIN, date of expiry and card status (normal, stolen, lost, blocked, hot etc).

iii) Routing of on-us and remote on-us transactions to Core Banking System; off-us transactions (transactions made by cardholders of other banks at bank's own ATM/POS) to a switch or credit card system of the issuing bank, or to a local/national payment network (NPSB, Q-Cash, Cash Link etc), or international payment network (MasterCard, VISA, American Express, Diners Club, Discover etc) for onward authorization,

iv) Fraud management,

v) Health monitoring of all the connected ATM and POS terminals,

vi) Settlement and reconciliation.

The standard Switching Software adheres to open system concepts and client/server or 3-tier architecture. The transaction processing engine resides on proven and robust UNIX platforms while the user and ATM device interfaces reside on Windows client workstations. System data is stored in an ANSI compliant relational database like Oracle.

In a typical environment, a switching system provides support to the hosted ATM/POS terminal, an ISO8583 interface to the Core Banking System or other bank's core banking system, and connectivity to regional, national or international networks. Other interfaces may include a host security module (HSM) for PIN verification, card output device (or card personalization system) for production of card, automated notification system for sending sms to the cardholders and ancillary applications for credit card, Call center etc.

The following switching software are in use in different banks in Bangladesh: IST/Switch of FIS Global Services (USA), iSwitch of Inter Block (Srilanka), CardSuite of Tieto Enator (Latvia), Phoenix of TPS (Pakistan), TranzWare of Compas Plus (Rissia) and ITM of Uronet (USA).

5.3. Credit Card Software

A Credit Card Software is a Credit Card transaction processing and management system which is used for the following specific purposes:

i) Production of **Credit Cards** which, in addition, includes insertion of customer's data into the system, and storing the inserted data into a database,

ii) Pre-authorization of on-us credit card transactions (transactions made by bank's own cardholders at bank's own ATM/POS) or remote on-us credit card transactions (transactions made by bank's own cardholders at ATM/POS of another bank). Note: pre-authorization includes validation of Card number, PIN, date of expiry and card status (normal, stolen, lost, blocked, hot etc) and final authorization includes debiting card limit.

iii) Authorization of the on-us and remote on-us credit card transactions.

iv) Routing of an off-us transactions (transactions made by cardholders of another bank) to the credit card system of another bank, or to a local/national payment network (NPSB, Q-Cash, Cash Link etc), or international payment network (MasterCard, VISA, American Express, Diners Club, Discover etc) for onward authorization,

v) Fraud management,

vi) Settlement and reconciliation.

The following Credit Card Software are in use in different banks in Bangladesh: TransMaster of Teito Enator (Latvia), CardPro of SunGuard (USA), iCard of Inter Block (Srilanka), TranzWare of Compas and CTL Prime of Card Tech (Cyprus).

5.4. Payment Gateway Software

A **payment gateway software** is a software that helps in authorizing payments for e-commerce transactions. It is equivalent of a physical POS terminal located in most retail outlets. Some of the main features of a payment gateway include:

- Software application designed especially for ecommerce, although it can be used to authorize payments in traditional brick and mortar businesses.
- Encryption of payment and personal data.
- Communication between the financial institutions involved and the business and the customer.
- Authorization of payments.

Some payment gateways feature tools that can help customers figure out shipping and handling costs, as well as sales tax. There are also fraud detection tools and other features that can be used with a payment gateway.

Functions of a payment gateway Software

A payment gateway software facilitates the transfer of information from cardholder to merchant portal (such as a website, mobile phone or IVR service) to acquiring bank to payment association to the card issuing bank. When a customer orders a product from a payment gateway-enabled merchant, the payment gateway performs a variety of tasks to process the transaction:

a) When a customer selects items to be purchased from the merchant's website and proceeds for payment by pressing the 'Checkout' or equivalent button, the payment gateway software at the bank to which the merchant's website is linked activates and the customer enters his card details.

b) The payment gateway then brings the transaction details from merchant's web-server to its own server located in the bank using SSL (Secure Socket Layer) encryption.

c) If the transaction is made by on-us card, the payment gateway forwards the transaction information to the Core Banking System (if debit card) or to the Credit Card System (if credit card) of the bank.

d) If the card is off-us (or not on-us), the payment gateway forwards the transaction information to the card association (i.e., Visa/MasterCard).

e) If an American Express or Discover Card was used, then the processor acts as the issuing bank and directly provides a response of approved or declined to the payment gateway.

f) Otherwise, the card association routes the transaction to the card issuing bank.

g) The card issuing bank receives the authorization request and sends a response back to the payment gateway via card association with a response code. In addition to determining the fate of the payment, (i.e. approved or declined) the response code is used to define the reason why the transaction failed (such as insufficient funds, or bank link not available)

h) The payment gateway receives the response, and forwards it on to the merchant website (or whatever interface was used to process the payment) where it is interpreted as a relevant response which is then relayed back to the cardholder and the merchant.

i) The entire process typically takes 2–3 seconds

j) The merchant close a "batch" of transactions made by different customers in an interval for settlement purpose. Bank only make settlement for the closed batches.

k) During settlement, the payment gateway checks and deposits the total of the approved funds in to the merchant's account. This could be an account with the acquiring bank if the merchant does their banking with the same bank, or an account with another bank.

In the above process, serial number (a) to (d), (h) and (j) to (k) narrates the functions of a payment gateway software.

Many payment gateway software also provides tools to automatically screen orders for fraud and calculate tax in real time prior to the authorization request being sent for authorization. Tools to detect fraud include geo-location, velocity pattern analysis, delivery address verification, computer finger printing technology, identity morphing detection, and basic AVS (Address Verification System) checks.

There is a growing support by acquirers, issuers and subsequently by payments gateways for Virtual Payer Authentication (VPA), implemented as 3-D Secure by VISA, SecureCode by MasterCard and J/Secure by JCB, which adds additional layer of security for online payments.

In Bangladesh Dutch-Bangla Bank has launched the country's first payment gateway software in the brand name of "Nexus Gateway" on 3rd June, 2010. The software named "Card Suit E-Commerce" has been procured from the Tieto Enator, Latvia. The Nexus Gateway accepts DBBL's Nexus Cards, debit and credit card suits of MasterCard and VISA (issued by any bank in the world). Thereafter BRAC Bank launched its internet payment gateway at the end of year-2010.

5.5. Software for Mobile Financial System

A Mobile Banking Software or Software for Mobile Financial System (MFS) is an application used by a bank to register mobile users, agents and merchants; authorize and record cash-in, cash-out, P2P, P2B, B2P, P2G, G2P and ATM transactions.

The P2P, P2B, B2P, P2G and G2P stand for Person to Person, Person to Business, Business to Person, Person to Government and Government to Person respectively.

First MFS of the country was lunched by Dutch-Bangla Bank as "Rocket" on 31 March, 2011 followed by "bKash" of Brac Bank.

5.5.1. Mobile Banking System Vs Core Banking System

The following are the main differences between a core banking system and a mobile banking system:

Items	Core Banking System	Mobile Banking System
Account Number	Conventional bank account number (with one check digit)	Mobile number + a check digit (optional)
Customer registration	By bank officer at branch	Input of mobile number by agent, data entry by bank/3rd party, and authorization by bank officer after verifying KYC.
Communication media	WAN (Fiber Optic, Radio Link, VSAT etc.)	Mobile network (sms/USSD) and/or WAN/internet
Posting device	Computer	Mobile Phone and/or Computer
Cash-in	By bank's Teller at branch	By bank's Teller at branch and by Agent
Cash-out	By bank's Teller at branch and at ATM	By bank's Teller at branch, by Agent and at ATM
No of transactions in a period	A few	Huge
Amount per transaction	Large	Small
Customer reach	Around the branch	Through-out the country

5.5.2. Mobile Banking system Vs sms Banking system

Mobile Banking system is not a sms Banking system. The main differences between the two systems are given below:

Particulars	**Mobile Banking System**	**Sms Banking System**
The customers access:	Mobile wallet / Mobile account	Bank Account (Savings, CD, STD etc)
Cash transactions?	Possible through Agents, Bank branch or ATM	Not possible
Device used by the customer to access the system:	Mobile set or ATM	Mobile set only
Connectivity between the Customer and the Bank's data center	sms, USSD, UTK, STK or BREW	sms only
Merchant payment	Possible	Not possible
Utility bill payment	Possible	Possible
3rd party (P2P) transfer	Possible, but not permitted in Bangladesh	Possible, but not permitted in Bangladesh

Note: sms stands for Short Messaging System, USSD for Unstructured Supplementary Services Data, UTK for UIM Tool Kit (where UIM = User Identity Management), STK for SIM Tool Kit (where SIM = Subscribers Identity Management) and BREW stands for Binary Runtime Environment for Wireless.

5.5.3. Available Software for Mobile Financial System (MFS)

In Bangladesh, Dutch-Bangla Bank, for the first time, started Mobile Banking services on 31 March, 2011 using the software named Sybase Mobilizer. BRAC Bank has selected the Fudamo as their mobile banking platform. Commercially available mobile banking software are listed below:

Name of the software	Developer
1. Rocket	Dutch-Bangla Bank
2. Sybase Mobilizer:	Sybase 365, Germany (now, acquired by SAP, USA)
3. Comviva:	Comviva Technologies Ltd., India
4. mCheck:	mCheck Limited, India
5. Fudamo:	Fundamo Limited, South Africa
6. Obopay:	Obopay, Inc., USA

7. bKash	Huawei Fintech Solution
8. Nogad DFS	Kona Software Lab

5.5.4. Customers of Mobile Banking / MFS and menu items for them

Three types of customers are involved in mobile banking. They are consumer, agents and merchants.

Consumer:

The consumers are the mobile phone owners who are registered for mobile banking services. In their mobile device, they will find the following menu:

- Balance Check
- Mini Statement
- Fund transfer (P2P)
- Utility Bill Payment
- Tuition fee payment
- Mobile Topup
- Change PIN

Agents:

The agents are Bank nominated parties who will perform Customer registration and cash transactions on behalf of the bank. In their mobile device, they will find the following menu:

- Customer registration
- Cash-in
- Cash-out

Merchants:

The merchants are Bank nominated shop owners who will sale their goods and services and receive payment from the customers mobile wallet into their own mobile wallet. In their mobile device, they will find the following menu:

- Merchant Payment

5.5.5. Features of a Software for Mobile Financial Services (MFS)

A Mobile Banking Software should have the following features:

- Provide connection to the mobile users, agents and merchants via a mobile operator using sms, USSD, UTK, STK or BREW. The sms stands for Short Messaging System, USSD for Unstructured Supplementary Services Data, UTK for UIM Tool Kit (where UIM = User Identity Management), STK for SIM Tool Kit (where SIM = Subscribers Identity Management) and BREW stands for Binary Runtime Environment for Wireless.

- Provide facilities to perform following activities by Agents, Consumer or Merchants:
    - Consumer, Agent and Merchant Registration
    - Cash : Cash-in/Cash-out through Agents, Bank Branches and ATMs
    - P2P: Fund Transfer from one customer's mobile account to the mobile account of another customer
    - P2B: Utility Bill payment, Tuition fee payment, Mobile TopUp, Merchant payment, Buying Bus/Railway/Airline ticket, Cinema Ticket
    - B2P: Salary disbursement by corporate bodies / Industries / Office, Remittance uploading
    - G2P: Disbursement of government elderly allowances, freedom fighter's allowances etc.

- Other features:
    - Audit trail
    - Maker & Checker
    - PIN verification if interface is ussd / stk / utk / brew.
    - If interface is sms, PIN verification through IVR
    - sms for some Mobile Network Operators (MNO) and ussd/stk/utk/brew for some other MNOs
    - All transactions need to send confirmation message to the customer by sms
    - Revenue sharing between parties such as Bank, Agent and MNO
    - Merchant Commission deduction from Merchant payment and sharing between Bank and MNO
    - vat deduction at the month end by the system
    - Fee and charge definition for different services
    - Interest calculation on deposit accounts

- Credit facility to the Agents and interest calculation
- End of Day processing

5.6. Agent Banking Software

5.6.1. Software for Agent Banking System

Agent Banking is the biometric authentication based banking software in which all transactions are validated by the fingerprint authentication. All the core banking system facilities are provided to the customers of agent banking. To spread the banking facility to the remote areas where the conventional banking services are not available, Agent Banking was introduced targeting that group of customers.

Agent Banking Software is an application used by banks to open accounts for consumer, agents and merchants; authorize and record cash-in, cash-out, fund transfer, bill payment, salary disbursement, ATM, eComm transactions.

Through this software, almost all the services are provided mainly by the bank nominated agent outlets. The agent banking customers can also avail specific services from the bank branch.

5.6.2. Agent Banking System Vs Core Banking System

The following are the main differences between a core banking system and a mobile banking system:

Items	**Agent Banking System**	**Core Banking System**
Account Number	Conventional bank account number (with one check digit)	Conventional bank account number (with one check digit)
Customer registration	➢ Input by agents through POS Device/ Desktop Application, ➢ KYC entry by Agent/Teller, ➢ Authorization by bank officer in Agent Banking Office after verifying KYC.	By bank officer at branch

Items	Agent Banking System	Core Banking System
Communication media	➢ For POS: Protected Mobile Data ➢ For Desktop App: Internet with secured VPN	WAN (Fiber Optic, Radio Link, VSAT etc.)
Posting device	➢ Biometric POS ➢ PC / Laptop	Computer
Cash-in	➢ By bank's Teller at branch ➢ At Agent Outlet	By bank's Teller at branch
Cash-out	➢ By Bank's Teller at branch ➢ At Agent Outlet ➢ At ATM	➢ By bank's Teller at branch ➢ ATM
No of transactions in a period	Huge	A few
Amount per transaction	Medium	Large amount
Customer reach	Through-out the country	Around the branch

5.6.3. Agent Banking System Vs Mobile Banking System

Items	Agent Banking System	Mobile Banking System
Account Number	Conventional bank account number (with one check digit)	Mobile number + a check digit (optional)
Customer registration	➢ Input by agents through POS Device/ Desktop Application ➢ KYC entry by Agent/Teller ➢ Authorization by bank officer in Agent Banking Office after verifying KYC.	➢ Input of mobile number by agent, ➢ Data entry by bank/3rd party, ➢ Authorization by bank officer after verifying KYC.
Communication media	➢ For POS: Protected Mobile Data ➢ For Desktop App: Internet	Mobile network (sms/USSD) and/or WAN/internet

	with secured VPN	
Posting device	➢ Biometric POS ➢ PC / Laptop	Mobile Phone and/or Computer
Cash-in	➢ By bank's Teller at branch ➢ At Agent Outlet	➢ By bank's Teller at branch ➢ At Agent Point
Cash-out	➢ By Bank's Teller at branch ➢ At Agent Outlet ➢ At ATM	➢ By bank's Teller at branch, ➢ At Agent Point ➢ At ATM
No of transactions in a period	Huge	Huge
Amount per transaction	Medium	Small
Customer reach	Through-out the country	Through-out the country

5.6.4. Type of Devices with Agent Banking System

The core of Agent Banking Software is the biometric authentication module as the transactions are accomplished on prior validation of fingerprint. For the authentication purpose, different types of devices are used to capture fingerprints of customers and agents on the basis of transaction type.

Device	**Description**	**Manufactured by**
Biometric POS	This is a POS device with inbuilt Fingerprint Scanner module., called as Biometric POS.	✓ Verifone ✓ Ingenico ✓ PAX
Fingerprint Scanner	Fingerprint scanner devices are used along with computers for capturing fingerprints.	✓ Secugen ✓ AbeTree ✓ Morpho ✓ Dermalog

5.6.5. Security

Beside common network, system related security for Banking system, Agent Banking Software ensure some application level security.

Biometric POS Device	➢ Registered Devices are binded with specific users so that no other can access that device. ➢ All the requests and responses are transmitted with gateway in encrypted format.
Desktop Application	➢ New Device Registration Requests are initiated by an agent with authentication of PIN, OTP to the registered mobile phone. ➢ Bank Admin needs to approve the newly added devices for further operation by users. ➢ Only the registered devices can be accessed by the mapped users after approval. ➢ All the requests and responses are transmitted with encryption. ➢ RSA Authentication is required at the time of user login.

5.6.6. Available Software for Agent Banking System

Different software companies provide the Agent Banking solution. As Agent Banking System provides the services of Core Banking System, many Core Banking System develper provides the software for Agent Banking.

Name of the Software	Clients
DBBL Agent Banking Software (In-house)	➢ Dutch-Bangla Bank
Agent Banking System, Era-InfoTech	➢ Bank Asia ➢ United Commercial Bank ➢ Shahjalal Islami Bank ➢ NRB Bank

	➢ Prime Bank ➢ Southeast Bank ➢ City Bank ➢ Jamuna Bank ➢ Sonali Bank
Integrated Agent Banking Solution (IABS) Islami Bank (In-house)	➢ Islami Bank
mFino, India	➢ BRAC Bank
Celloscope, Bangladesh	➢ NRBC Bank ➢ Agrani Bank
Millennium Information Solution, Bangladesh	➢ Al-Arafah Islami Bank ➢ Social Islamic Bank Ltd
Micro Solutions, Bangladesh	➢ Mercantile Bank
Flora Agent Banking System Flora Systems, Bangladesh	➢ Midland Bank ➢ One Bank ➢ South Bangla Agriculture & Commerce Bank
Easy Bank (In-house)	➢ Eastern Bank
Modhumoti Digital Banking Datasoft, Bangladesh	➢ Modhumoti Bank
nCore, Leads Corporation	➢ Premier Bank

5.6.7. Customers of Agent Banking and menu items for them

Mainly two types of customers are involved in Agent banking. They are consumers and agents.

Consumer:

Consumers are not able to access the system directly if the bank does not provide any customer fetching application i.e. mobile apps, internet banking etc.

Agents:

Bank nominated agents are the main transaction initiators who will perform Customer registration and cash transactions on behalf of the bank. In their Biometric POS or Desktop Application, they will find the following menu:

- Customer Registration
- Cash-in
- Cash-out
- Fund Transfer
- Bill Payment
- Balance Check
- Statement Check

5.6.8. Features of a Software for Agent Banking Services

- **Registration Process**
  - Registration of Super-Agent, Agent, DSR, Sub-Agents, FT officer, ROs and Teller
  - Registration of New customers
  - Linking of Core Banking Customers
  - Biller Registration
  - Change of Fingerprint
  - Replacement of Agent/Sub-Agent
  - Agent Hierarchy Management

- **Services**
  - Cash-In & Cash-Out

- ❖ Utility Bill Payment
- ❖ Balance & Statement Check
- ❖ Fund Transfer
- ❖ ATM Transaction
- ❖ POS & eCOM Transaction
- ❖ Salary Upload
- ❖ Loan Disbursement
- ❖ Fund Management by Agent Hierarchy
- ❖ Remittance through agent points and branches

- **Other Operations**
  - ❖ All transactions need to send confirmation message to the customer by SMS
  - ❖ End of Day processing
  - ❖ Distribution of Commission to Agent Hierarchy
  - ❖ Payment of “Commission on Float” to Agent & Sub Agent
  - ❖ Service Charge, Interest & Limits
  - ❖ VAT deduction at the month end by the system
  - ❖ Fee and charge definition for different services
  - ❖ Interest calculation on deposit accounts
  - ❖ Revenue sharing between parties i.e Bank, Agents

Review Questions

1. Multiple Choice Questions (MCQ)

i) Recommended temperature for a Data Center is ….. degree C and humidity is ….. %

a) 10, 38 b) 20, 70 c) 25, 50 d) 20, 50

ii) Higher data transfer rate is found in ……

a) LAN b) Internet c) WAN d) VSAT

iii) A router is used in …..

a) LAN b) Internet c) WAN d) Hard Disk

iv) A VSAT is used in …..

a) LAN b) Internet c) WAN d) Router

v) The largest WAN is ……

a) ICT Ministry Network b) Facebook network c) Internet d) SWIFT

vi) The most popular implementation of RAID is level …..

a) Level-5 b) Level 0 c) Level 1 d) Level 0+1

vii) Which of the following is not a part of LAN?

a) Router b) Network Switch c) LAN d) Computer

viii) Which of the following is not a transmission media of LAN?

a) Coaxial Cable b) Wi-fi c) Fiber Optic Cable d) VSAT

ix) Which of the following is the transmission media of WAN?

a) Microwave b) Wi-fi c) Coaxial Cable d) Twisted-Pair Cable

x) Firewall is used in a WAN for which of the following?

a) Additional Bandwidth b) Additional Security

c) Additional distance d) Additional Accuracy

xii) Where a Dark Fiber is used?

a) Between DC and DRS b) In a wi-fi

c) Between LAN and WAN d) In computer programming

xiii) Why a SAN switch is used?

a) To connect Servers with a Storage
b) To connect WAN and LAN
c) To connect two cities
d) To connect two bank branches

2. Fill in the Gap(s)

i) The run length of individual Ethernet Cables in LAN is limited to roughly ….. meters.

ii) LAN follows either …… or …… architecture?

iii) For setup of an ICT infrastructure of a bank having 50 branches, the approximate budget requirement is Taka …… million.

iv) In the LAN-based approach of bank automation, ---- or Novel operating systems was used. The data was stored in a server as flat file or database either ----- or dBase. The application software was written in ……, …… or dBase.

v) Nexus Gateway was lunched for the first time in Bangladesh by Dutch-Bangla Bank in the year of ……

vi) Rocket was the first MFS in Bangladesh launched by Dutch-Bangla Bank on ……

vii) Near Data Center is a Data Center established in the same city where ----- is located.

viii) The DRS should have capability to become primary site automatically in case the ---- is in disaster.

ix) One of the common data center certification awarded by the “Uptime Institue” is ----- certification.

x) A WAN connects two or more --------.

xi) The largest WAN in existence is --------.

x) Bandwidth of a VSAT is ---- than that of Radio Link.

xi) DMZ in Computer Networking stands for --------.

xii) In the 3-tier architecture of computer programming technique, normally user's computer termials, application server and ------ are involved.

xiii) P2G stands for ----------.

Probable Questions

1. What is a Data Center? What are the basic requirements of a Tier-4 Data Center?

2. Why near Data Center is important for FIs?

3. Why FIs setup DRS? What points need to be considered during selection of distance between a DC and a DRS?

4. Narrate advantage and disadvantages of Tier-1, Tier-2, Tier-3 and Tier-4 data centers.

5. What is LAN card? Why it is needed in a LAN?

6. Name 3 LAN and 3 WAN communication media.

7. Mention a few of the differences between LAN and WAN?

8. Describe advantages and disadvantages between the following data transmission media for a WAN of a Bank: Land Line, Microwave and Satellites.

9. Why Firewall is installed in the networking system of a bank?

10. Why DMZ needed to be established in the network system of a bank?

11. Narrate functions of a branch server, application server and database server.

12. What is the 3-tier architecture of computer programming?

13. What is RAID? Why RAID is used in Banking system?

14. What are the differences between a RAID level 0 and 1? What do you mean by RAID level 0+1?

15. What do you mean by computer clustering? Why clustering is used in a computer system of a bank?

16. Define replication with an example.

17. What is dark fiber cable and where is used in a banking system?

18. Why a banking system uses external storage instead of an internal storage for storage of its data?

19. Define SAN switch.

20. Why database backup is important in banking?

21. What are the three types database backup? Explain each of them. Which one is suitable for your bank/FI?

22. What do you mean by Alternative Delivery Channel?

23. Mention some disadvantages of a stand alone approach of bank automation.

24. Narrate history of online banking in Bangladesh.

25. Mention 3 functions of each of the following software: a) Core Banking Software, b) Switching Software, c) Credit Card Software, d) Payment Gateway Software.

26. Why each of the following software are used in Banks? - a) Core Banking Software, b) Switching Software, c) Credit Card Software, d) Payment Gateway Software.

27. What are the main features of a Payment Gateway Software?

28. What are the differences between Mobile Financial System (MFS) and Core Banking System (CBS)?

29. What services are available in Agent Banking System?

30. Which additional features other than the features in a core banking software should be available in Agent Banking Software?

31. What are the differences between a Core Banking and Agent Banking System?

32. List special devices required for Agent Banking operation.

33. What kind of application level securities to be incorporated in Agent Banking System?

34. Name 5 (five) Agent Banking Software available in Bangladesh.

35. What menu a customer gets to operate Agent Banking?

Module-C

Alternative Delivery Channels & Funds Transfer Systems

Alternative Delivery Channels are channels other than traditional branch networks using which different banking services are delivered to the bank clients. These channels include ATMs, CRMs, Deposit Machines, POS terminals, Internet Banking, sms alert Banking, e-commerce, Call Centre, Mobile Financial system (MFS) and Agent Banking.

For sending fund transfer instructions, many devices/systems are used. These are Telex, SWIFT, BACH, BACPS, BEFTN, NPSB, RTGS, CHIPS, FEDWIRE, BANKWIRE etc.

In this module we will discuss various Alternative Delivery Channels and Fund Transfer Systems.

1. Automated Teller Machine (ATM) and Cash Recycling Machine (CRM)

ATM/CRM is used for cash withdrawal (ATM/CRM) and Cash deposit (CRM only) operations with a bank card. Besides, the ATM/CRM allows the holder of a card to receive the information on the current status of the account (including an extract on a paper), and also to transfer money from one account to another. Obviously, the ATM/CRM is supplied with the device for reading a card, and with the display and the keyboard for interaction with the card-holder. The ATM/CRM dispenser is equipped with the personal computer which provides management of a cash dispenser and the control of its status. The last is rather important, as the cash dispenser is storehouse of cash. Monetary denominations in an ATM/CRM are placed in cassettes which are in the special safe. The number of cassettes defines number of the denominations which are given out by an ATM/CRM and receive by an CRM. For maintenance of communication functions ATM/CRM is equipped with modems or LAN Card.

Figure: An ATM

The use of ATM/CRM in Bangladesh is limited to urban cities only. The number of ATM/CRM in Bangladesh is increasing rapidly, the number increased from 100 in 2003 to 1900 in 2010 to 11,000 in 2021. Out of 11,000 ATM/CRM, Dutch-Bangla Bank installed 5,000 ATM/CRM alone. Next large ATM/CRM acquirers are BRAC Bank, Islami Bank and Q-Cash network.

1.1. Services from ATM/CRM

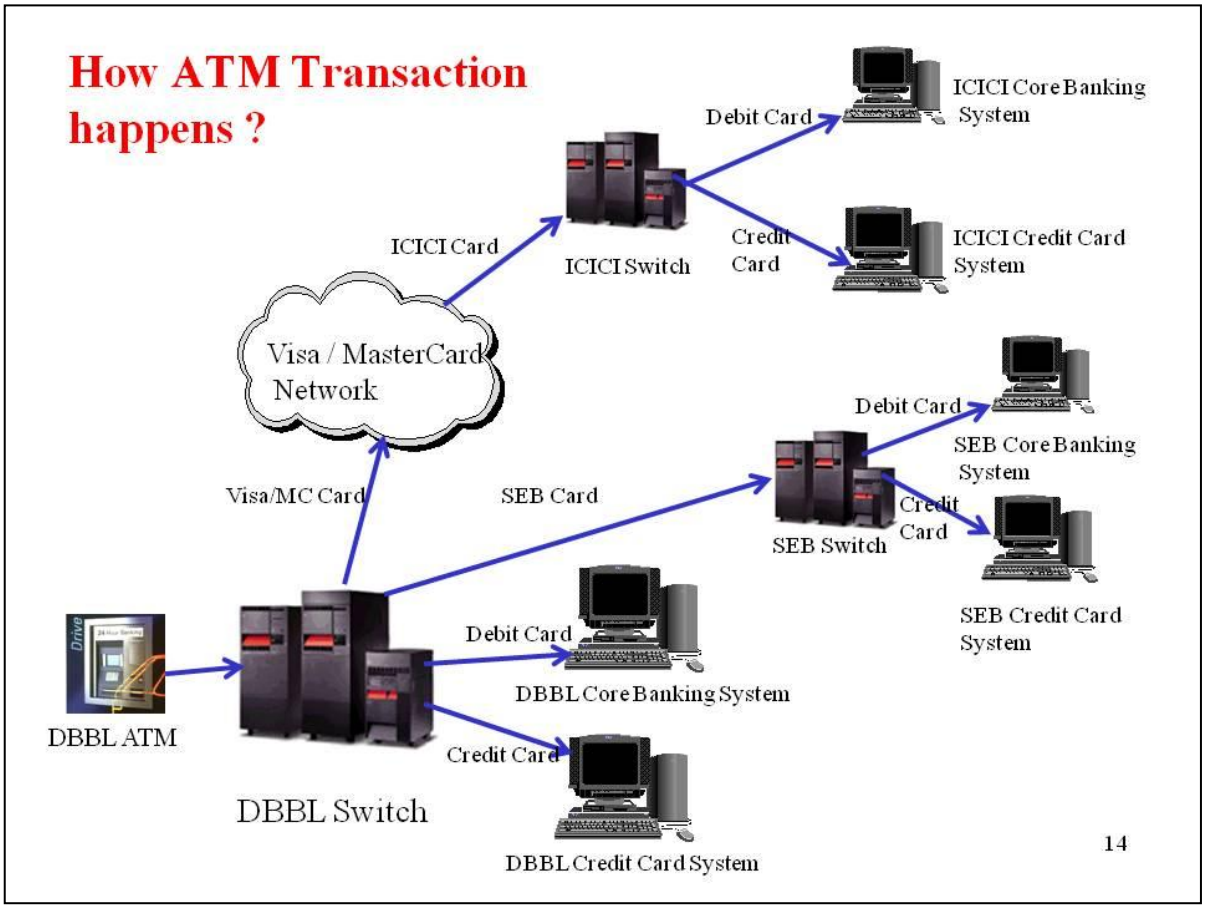
The cardholders can perform many banking activities using an ATM/CRM as listed below:

- Cash withdrawal
- Cardless cash withdrawal
- Cash deposit (CRM only)

- Fund transfer from one account to another
- Interbank fund transfer
- Receiving foreign remittance
- Balance enquiry
- Printing Statement of account
- Cheque book request
- Utility Bill Payment
- Mobile recharge

1.2. How ATM/CRM works in case of cash withdrawal?

All ATMs/CRMs are connected to a Switching Software at Data Centre of the Bank. When a card is inserted into the ATM/CRM, the card reader reads card number, date of expiry, banks identification number etc from the Meg-stripe or Chip of the card, take user input for PIN and amount to be withdrawn, and passes these information to the Switching Software.



The Switching Software then checks if the card is on-us or off-us. If on-us and the card is a debit card, the Switching Software checks the validity (card number exists in the database, date does not expire etc), status (not a stolen or hot card) and PIN of the card. If all the checks are passed,

the corresponding account number and amount are passed into the Core Banking system of the Bank with a request to make debit in the account. If the Core Banking System found adequate balance in the account and the account is otherwise operative, it debits the account for the amount, and send an authorization code to the ATM/CRM via Switch. ATM/CRM, then count the money and presents to the customer.

If the card is on-us and a credit card, the Switch does not check anything but pass the information to the Credit Card System. The Credit Card System checks the validity (card number exists in the database, date does not expire etc), status (not a stolen or hot card) and PIN of the card. If all the checks are passed, and the Card account has sufficient available credit limit, the Credit Card System debits the card account for the amount, and send an authorization code to the ATM/CRM via Switch. ATM/CRM, then count the money and present to the customer.

If the transaction is not on-us, the Switch checks if the transaction is made by a cardholder of a bank in Bangladesh. If the Cardholder belongs to a bank in Bangladesh, the pass into the National Payment System, Bangladesh (NPSB) of Bangladesh Bank (Central Bank). NPSN passes the transaction to the switching software of the cardholder's bank. The Switching Software of the Bank verifies the card validity, status, PIN etc and obtains authorization code from the Core Banking System (if debit card) or Credit Card System (if credit card) and passes this code to the ATM/CRM via NPSB and Switch of the acquiring bank.

If the transaction is not on-us and the card is an international one, it forwards the transaction to the appropriate payment association (Visa, MasterCard, JCB, Union Pay etc). The payment association forward the transaction to its member bank, the Switch of which verifies the card validity, status, PIN etc and obtains authorization code from its Core Banking System (if debit card) or Credit Card System (if credit card) and passes this code to the ATM/CRM via payment association and Switch of the acquiring bank.

If the authorization code is positive, the ATM/CRM counts the money and present to the customer.

1.3. ATM/CRM Specifications & related topics

1.3.1 ATM/CRM specification

ATM Types: In Bangladesh two types of ATMs are available - Lobby type and Through-The-Wall type. The Lobby type ATM requires small space to install, whereas the Through-The-Wall type of ATM requires large space with two compartments in a room. Front part is used for customers and has a separate door and Air conditioning (AC) system. The back side is machine room and also has a separate door and AC. The cash is loaded from the rear side. In case of a Lobby type ATM, cash is loaded from the front side of the ATM and requires only one room with one unit of AC.

ATM/CRM Manufacturers: The top four brands of ATMs/CRMs are: Diebold, NCR, Hitachi, Wincor-Nixdorf.

Figure: A NCR ATM, a Diebold ATM and a Wincor-Nixdorf ATM

Computer: Each ATM has a computer in it. A latest processor is used for the computer. One GB RAM, 80 GB HDD, 10/100 Base T Ethernet USB, Ethernet Adapter are integrated with the computer. The computer starts the ATM, stores journal records electronically, and communicate with the Switch using TCP/IP on leased line, GSM and V-SAT network with **3DES** chip Encryption / verification / validation.

Display: 15" / 17" color display – LCD or Touch Screen.

Card Reader: The card reader is very important parts of an ATM/CRM. It reads the customers card either from meg-stripe or from the Chip (if EMV card).

Protocol: Two protocols – NDC+ and D912 are used to communicate with the switch.

Key Pad: Encrypted / EPP (PCI Compliant) Standard keyboard with functional keys are used with ATM/CRM.

Printers: Two printers – a Consumer Printer and a Journal Printer are provided with an ATM. The consumer printer prints the slip after every transaction for the customers whereas the Journal Printer resides inside the ATM/CRM and prints all the transactions with fail / successful status. The disputes on cash delivery can be identified from this journal. Now a day, this paper journal has been replaced by a electronic journal.

Dispenser: Dispenser is a unit which counts and dispenses money. Dispenser uses vacuum pick or Friction Pick technology for counting and dispensing money.

Security: ATM/CRM vaults are provided with dual combination lock, as two officers are required to open the vault. The safe is available in 2 standards – UL291 and CEN. CEN is stronger than UL291.

Accepting cash at CRM: CRMs have cash deposit option. The cash is deposited as bundle. The CRM counts the cash in different denominations and re-fills the dispensing cassettes. Thus requirement of number of cash feeding at CRM is much lower than that in ATM.

1.3.2. Denomination available at ATM/CRM

Number of denomination available in ATM/CRM depends on the number of cassettes that can be inserted in an ATM/CRM. If there are provision for housing 4 cassettes in an ATM/CRM, 4 types of currency notes can be loaded. However, to avoid frequent cash loading, the banks normally provide only one or two denominations in the ATM/CRM, like Taka 1000 notes in 2 cassettes and Taka 500 notes in another 2 cassettes. A cassette can hold 2000 notes. Thus if two cassettes are loaded with Tk.500 notes and another 2 cassettes with Tk.100 notes, total amount of taka that can be loaded into an ATM/CRM at a time is Tk.2.20 million.

1.3.3. Cash feeding by 3rd party

With a size of 1000 ATM and 1 million cards, a bank needs to load Tk.500 million everyday in the ATM. This amount is much less in cash of CRM. Sometimes it may require to remove cash from the CRM if amount of cash deposit is more than cash withdrawal.

As the quality of note in our country is not good and note contains holes, before cash feeding into an ATM, it is required to check all the notes one by one, reject the bad notes manually and then arrange the notes in such a way that the hole of two adjacent notes fall in two opposite sides. This requires a huge manpower every day. Thus this job is outsourced to 3rd party. However, this activities has been reduced substantially if CRMs are installed instead of ATMs.

1.3.4. Partial Dispense of Cash and non-dispense of cash

Sometimes due to error in dispenser or bad note quality, the ATM/CRM can't count all the notes requested by the customer. In such case ATM/CRM either dispenses part of the money or none. In such a case, normally the ATM/CRM sends a reversal request to the authorizer via Switch and the authorized credit the non-dispensed amount into the customer account.

Sometime, the reversal also fails and thus customer finds less money in his account. The cardholder, in such case, must report to the card issuing bank. The cardholder is not known to

the acquiring bank, acquiring bank does not have access to the customer account, and thus they can't take any action in this regard.

1.3.5. Capture of money

After money is presented to the customer, the ATM/CRM beeps and waits for 45 seconds (configurable). If the customer does not receive money within this time period, the ATM/CRM captures the money and keeps in a cassette called "reject bin".

1.3.6. Network used for connectivity

The ATM/CRM requires a small bandwidth to complete a transaction, only 16 Kbps. Thus any type of communication media can be used for ATM/CRM transaction. Most easy and cheap media for ATM/CRM transaction is mobile data network. However, banks normally use fiber optic for data connectivity as this is most reliable media for communication.

1.3.7. Card Capture and hot card

For security reason, if a cardholder inserts wrong PIN 3 times, the ATM/CRM captures the card and the card become hot. In such case the customer should report to his home branch. The cash loading team, during their next visit, will collect the card and send to the acquiring bank. If a hot card is inserted into the ATM/CRM, the ATM/CRM will capture the card immediately. Therefore, it is required to call to the help desk of the bank and make the status of the card normal before using a hot card. During your call the bank officer may ask you several questions to be sure that you are the cardholder. Other reasons for capturing cards are: power failure (or UPS backup exhausted) at ATM/CRM, card was blocked earlier, problem of cards reader of the ATM/CRM.

1.3.8. One-time and monthly expenditure for an ATM/CRM booth

The one-time investments in an ATM/CRM booth are as follows:

- Price of ATM/CRM
- Advance to the landlord
- Price of UPS, CCTV, Air Conditioner
- Cost of construction of booth, signage and decoration

The monthly recurring expenditures are as under:

- Rent of the booth
- Electricity cost
- Salary of 3 Security Guards engaged in 3 shifts
- Cash sorting and feeding charge
- Link charge

- Maintenance charge for ATM/CRM, UPS, CCTV, AC and booth
- Proportionate Switching System cost
- Proportionate Data Centre manpower and maintenance cost

The one-time cost may vary from Taka 2.00-2.50 million and the monthly recurring cost may vary from Taka 80,000 - 100,000 per ATM/CRM.

1.3.10. Income from an ATM/CRM

Normally there is no transaction fee for the on-us transaction at ATM/CRM. However, for the off-us transactions, the Acquiring Bank receives Tk.20 for each local transaction and USD1.00-1.25 for each international transaction. This is called local and international ATM/CRM interchange fee respectively, and determined by the Bangladesh Bank and respective payment associations. Annual fee on the debit card charged to the cardholders may also be considered as fee income.

1.4. ATM/CRM Fraud and remedy

ATM/CRM fraud throughout the world has increased significantly over the past few years and is becoming more sophisticated, incorporating technologies to record bank card and PIN information.

ATM/CRM fraud generally comes in two varieties: card-reading devices and card-trapping devices.

1.4.1. Card Reading Devices

Criminals alter the ATM/CRM itself by adding a skimming machine and a mini-camera to it. The skimming device, mounted on the card entry slot, reads the bar code of the card. The mini camera records PIN as the cardholder enters his PIN. After the cardholder completes his transaction, receive card, and walk away, someone else has his card information and his PIN. Usually, the fraudster makes a new card and uses it to withdraw money from the customer's account. The skimming devices are not always easy to spot, especially if the customers are unfamiliar with the look of ATMs/CRM.

Now a day all the ATMs/CRMs come with anti-skimming device which crates vibration while card is inserted. This vibration prevents reading and recording of card information by the skimmers by installing a skimming machine. If the older ATMs/CRMs doesn't have anti-skimming device installed on it, Banks should buy separate anti-skimming devices and integrate with the ATM/CRM.

A normal ATM device.

ATM with skimming device attached in front of card slot. Notice how the card slot is no longer inset into the machine, but "bulges" outward.

1.4.2. Card-Trapping Devices

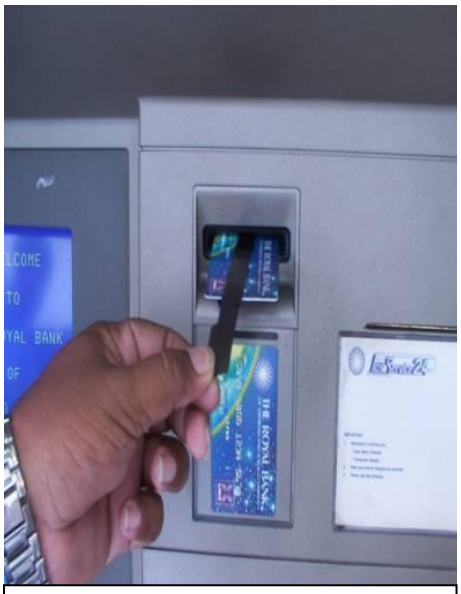


Figure: A card trapping device

An alternative form of altering the ATM/CRM itself involves inserting a thin ribbon of x-ray tape into the card slot. The loop traps the customer's card and makes it seem as though the card is not working. At this point, someone else, a fraudster comes along and tells the cardholder that he (cardholder) can retrieve his card by re-entering his (cardholder's) PIN code. The fraudster watches while the cardholder does so. After the card still refuses to emerge and the cardholder walks away from the ATM/CRM, the fraudster removes the device with the card, which he then uses to withdraw money from the cardholder's account.

In order to prevent becoming the victim of such scams:

- Customers need to avoid ATMs/CRMs where the card slots appear to have been mounted on the machine. Card entry slots should be flush with the surface of the ATM/CRM or recessed from it. If a customer sees a card entry slot that is raised above the machine, it should raise suspicions and should not be used.

- If the customer finds it awkward to read the screen or enter your PIN, he shouldn't use the machine. It may have been altered. Legitimate displays are never mounted in front of ATMs/CRMs. Anything that blocks or partially obscures a sign may house a camera.

- Customer needs to guard his PIN, especially when entering it, by shielding the keypad with one of his hands.

- If a machine swallows the card, customer need to call the bank's help desk and report it.

- Customer should change the PIN from the original number given when he first got his card. Customer shouldn't keep his card and PIN together.

- Banks should buy and install ATM/CRM having built-in anti-skimming devices. For old ATMs/CRMs where there are no anti-skimming devices integrated, bank may buy separate anti-skimming device and install in all such ATMs/CRMs.

2. Deposit Machine

A deposit machine is a machine installed by a Bank and used by the customers for depositing money into it. Deposit machine is also called as KIOSK. A deposit machine may have a card reader. If a cardholder sweeps his card before making a deposit, he does not require to type his account number or card number. The Deposit machine can recognize the customer. The amount to be deposited is inserted into a closed envelope and dropped inside the machine. The amount deposited needs to be key-in using the keyboard of the deposit machine.

Some time, the amount key-in and the physical amount inserted inside the envelope may vary. The envelopes are opened by a team within the coverage of CCTV. If dispute arises, the decision of the team (bank officials) will be final. However, if the customer disagree, the customer can view the CCTV record.

However, some banks, to avoid such disputes, engaged bank officers at each of the deposit machines to ensure amount inside the envelope. The envelope, before dropping into the deposit machine, should be signed by both the officer and the customer.

The important part of a deposit machine is vault, its specifications (UL or CEN) and its note capacity. The vault capacity can be as large as to accommodate 700 envelops containing 500 notes in each envelope.

The deposit machine is also equipped with a computer, monitor and software.

Locally manufactured deposit machines are available in Bangladesh.

3. Fast Track / Electronic Booth

Fast Track/Electronic Booth is a unique concept developed by Dutch-Bangla Bank for its customers. The following are installed in a Fast Track/Electronic Booth:

- Several numbers (5-15) of ATMs
- Several number (1-3) of CRMs/Deposit machines
- One officer each for two shifts
- Several UPS

- Links for several network providers

ATMs/CRMs are normally become out of order in the ATM booths due to the following reasons:

- No link with the bank server
- No money inside the ATM/CRM
- Cash jam due to soiled note which prevent withdrawing money by the next customers
- ATM/CRM hardware problem
- UPS is out of order
- No electricity

To arrest all the above problems, Dutch-Bangla Bank has installed Fast Track. BRAC Bank and Standard Chartered Bank have also installed Electronic Booth with the same concept.

The activities of a Fast Track/Electronic Booth are mentioned below

a) Cash Withdrawal:

Customers can withdraw money from any of the 2-5 units of ATMs/CRMs installed at Fast Track/Electronic Booth. The ATMs/CRMs are powered from different UPS and linked to Data Center through various link providers which created redundancy for power failure and network problem. Again due to multiple ATMs/CRMs at Fast Track, further redundancy has been ensured for ATM/CRM disorder, Cash shortage and Cash jam. This ensures that a customer will be able to withdraw money from ATM/CRM at Fast Track without failure. On the other hand, presence of an officer at FT helps the customer to solve any ATM/CRM related problem such as Cash/Card capture.

b) Cash Deposit

A customer can deposit money at Fast Track/Electronic Booth and avoid a long queue at the branch counter for depositing money. The customer can also get service for the extended hours from the Fast Track/Electronic Booth for depositing money. Customers can directly deposit money in the CRM or use deposit envelope having money inside it in the Cash Deposit machine. In case of cash deposit machine, the official on duty at Fast Track/Electronic Booth receives cash or cheque from the customers, counts, inserts into an envelope, closes the envelope, and puts a sign on it. The customers also sign on the envelope and drop it into the deposit machine. If CRM is used to deposit money, customer's account is credited instantly while if Deposit Machine is used, customer's account is credited next working day.

c) Account Opening

The officer on duty assists the customers to submit the customer's eKYC for account opening. The officer can handover the account number and debit card to the customer instantly. The customer can also deposit to his account using the CRM.

d) Customer Request Form

Various customer request forms are available at Fast Track/Electronic Booth. The duty offers provide the appropriate form to the customer, assist to fill-in the forms, receive the form from the customer and send to the relevant Division of the Head Office or branch for execution of the customer's request. A list of such services is given below:

i) Customers can fill-in a “Account Transfer” form and hand over to the Fast Track/Electronic Booth officer for fund Transfer to another account

ii) Customers can fill-in a “New Card” form and hand over to the Fast Track/Electronic Booth officer for getting a new Debit Card (MasterCard Debit / Maestro / Visa Debit/Visa Electron) or Credit Card (MasterCard / Visa)

iii) Customers can fill-in a “Card Replacement” form and hand over to the Fast Track/Electronic Booth officer for getting a replacement Card (Debit/Credit) for any of the following reasons:

- Card Lost / Stolen
- Incorrect name / spelling mistake on card
- Wrong photograph on card
- Card is physically damaged
- Magnetic Strip error/Faulty card
- Any other reason acceptable to Fast Track Officer

iv) Customers can fill-in a “Block/unblock Card” form and hand over to the Fast Track/Electronic Booth officer for blocking his Card / for reactivation of a blocked Card. Card may be blocked for any of the following reasons

- Incorrect PIN entered at ATM or POS terminal
- Customer blocked the card over a phone request to the Card Center
- Any other reason acceptable to Fast Track/Electronic Booth Officer

v) Customer can place a request for re-issue of PIN. Re-issue of PIN may be requested by a customer who have forgotten his PIN or in the fear that his PIN have been compromised to another person.

vi) Customer can place a request for linkage of a new account with his exiting card

vii) Customer can place a request for the following services on Credit Card account:

- Auto debit
- Increasing card limit
- Limit transfer

- Obtaining Supplementary Card
- Early renewal
- Cancellation
- Card Cheque
- Any other service acceptable to the Fast Track Officer

viii) Customer can place a request for refund of Cash not dispenses from ATM/CRM but account debited.

ix) Customer can submit application form for availing Internet, SMS & Alert facility on bank account.

e) Delivery of Captured Card

If a Card is captured into an ATM/CRM at the Fast Track/Electronic Booth, the duty officers open the upper chamber of the ATM and deliver the captured card to the cardholder instantly after checking his photograph and signature recorded at the back of the card.

4. POS terminals

4.1. What is a POS terminal?

POS stands for Point of Sale. POS terminal is a small device installed by a bank at shops, hotels and offices of a merchant. The customer buys the good and services from the merchant, and if wants to pay the bills using his debit/credit card, the merchant uses the POS device to swipe or insert the card for settlement of his bill.

POS terminals are intended for processing transactions at merchant locations with use of debit/credit cards with a magnetic strip and smarts-cards. Configuration of POS terminals vary over a wide range, however the typical modern terminal is supplied with devices for reading smarts-cards and magnetic strip, ports for connection of PIN PAD (or built-in PIN PAD), the printer, connection with the PC or with an electronic cash register.

Figure: A POS terminal

Besides usually the POS terminal is equipped with a modem with a capability to call-back. The POS-terminal can be programmed. This allows on-line authorization of cards. Finally, the communication is passed to Data Centre. During a session of connection, the POS terminal can accept and remember the information transmitted by the Server of the Data Centre.

A POS terminal can communicate with Data Center using PSTN line or GPRS. PSTN POS terminal requires a telephone line for communication whereas the GPRS POS terminals uses mobile SIM card for communication. When a card is swipe (in case the card is meg-stripe) or inserted (in case the card is EMV) the POS terminal dial to a set number and get connected with the modem pool of Data Center (called NAC – Network Access Controller). After connection, the exchange of information happens.

GPRS POS terminal has advantages over a PSTN POS terminal. A GPRS POS terminal can be moved anywhere as it has SIM and built-in battery.

4.2. Transaction types supported at POS terminals

A merchant can perform following transactions using a POS terminal:

Sale: Customer pays for merchandise or service from his/her account.

Void: Before end of day (Settlement), merchant can cancel the sale and give the money back.

Refund: After end of day (Settlement), merchant can cancel the sale and give the money back.

Pre-authorization: Merchant can block some amount of money from the customer's account for a specific time. It is usually used in hotels. Merchant guarantees to get money for the services.

Cash Advance: Customer can use POS to get money from the account. Merchant will give the money to customer instead of goods or service. This is like using POS as ATM to get the money from the account.

4.3. POS Specifications:

Brand: Three popular brands of POS terminals are: Hypercom, Verifone and Ingenico.

RAM: 2 MB – 8 MB Flash

Processor: ARM 32 bits / 32 bits RISC

Magnetic Card Reader: ISO 1/2/3

Smart Card Reader: EMV level 1 & 2 and ISO 1/2/3

Encryption: Triple DES

Printer: Thermal,

Display: Graphic, 128x64 pixels; Backlight

Communication: GPRS / PSTN

4.4. How POS works?

A POS transaction is a purchase that begins with a cardholder. The diagram below will help us better understand the transaction process. Essentially, the transaction process is a series of purchases, beginning with the cardholder:

a) The cardholder purchases goods or services from the merchant.

b) The merchant, in effect, sells the transaction to the "acquirer" and is reimbursed the amount of the sales ticket less a "discount fee."

c) The acquirer then submits the transaction to the issuing bank for payment via Central Bank's or Payment Association's (i.e., VISA, MasterCard etc.) interchange and settlement system.

d) The issuing bank pays the merchant acquirer, less an interchange fee which partially reimburses the issuer for its expense, through Central Bank's or Payment Association's settlement system.

e) Finally, the cardholder repays the issuer for the goods or services originally purchased from the merchant.

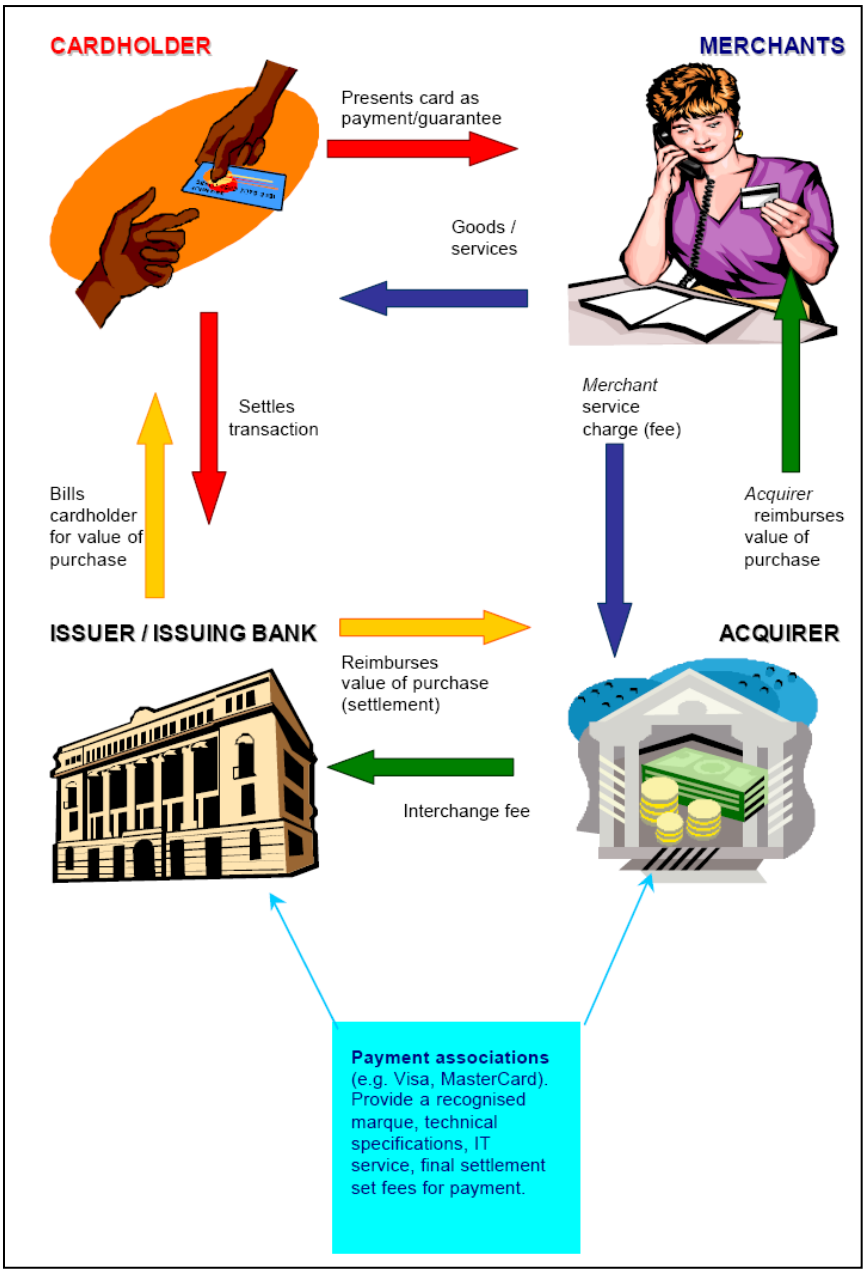


Figure: How POS terminals works

4.5. POS terminology

a) PIN pad:

A PIN pad is required with the POS terminal for cardholder to insert and encrypt his PIN. To accept Debit card at the POS terminal, the POS terminal must have separate or built-in PIN Pad.

b) Insert and Swipe:

A non-EMV card needs to be swipe in the POS terminal whereas an EMV card needs to be inserted in the POS terminal.

c) Merchant Commission:

A commission in percentage on the sale value, which the merchant pays to the bank that supplied the POS terminals. If a merchant sale an item at a cost of Taka 100 and the cardholder pays the bill using his card, the bank receives Taka 100 from the cardholder, but pay Taka 98 to the merchant, if the merchant commission mutually agreed is 2%.

d) Interchange fee:

Interchange fee for POS is the fee which acquiring bank pays to the issuing bank. This comes into picture if a cardholder of a Bank pays bills at a merchant location where the POS is supplied by another bank. The interchange fee is fixed by the central bank or payment associations, such as for MasterCard, this is, say 1.16%. In the above example, the acquiring bank will earn 2.0% commission, but as the cardholder is of another bank, the acquiring bank has to pass on 1.16% of the sale value to the issuing bank.

4.6. Fraud at POS and remedy

In the POS terminals, Counterfeit Cards are used for payment against purchase of goods which the fraudsters can easily sale in market (such as gold and electronic items) to get the cash in hand.

A counterfeit card is one that has either been created from scratch by criminals using real or fake card numbers or is a valid card that has been altered.

The majority of counterfeit card fraud finds its source from skimming, the process whereby legitimate card details are recorded from a card's magnetic strip and are subsequently encoded onto a fake card by the criminals. Skimming is normally perpetrated by retail staff who record card details using pocket sized recording units before returning the valid card to the cardholder during a sale. They then sell the recorded information to organized criminal groups, who make the counterfeit cards. However, the use of skimmed data is not limited to the production of fake cards for use in card present environments. The information is also used to undertake fraudulent card not present transactions (e-commerce transaction) with false delivery addresses.

Once the card data is in hand, the fraudsters produce a physical card with a bank name, his own name, picture and signature. However, inside the meg-strip, he uses the card information of the victim. After shopping when he places the card at the merchant, the merchant finds that the photograph and signature is perfectly matching. However, the POS has got another set of information. The POS will send this information to the acquiring bank, which will forward the

transaction to the victim's bank (issuing bank). The issuing bank will find everything in order and authorize the transaction. As such the merchant will hand over the items to the fraudster.

The merchant, after closing his POS batch, will get his money in his account from the acquiring bank. The acquiring bank will also get money from the issuing bank. However, when the cardholder will get his account statement, he will deny to pay this money as he has not made this transaction.

Investigation will start. One of these two banks will have to absorb the loss. If any of them is EMV compliant, it will win. If both the banks are non-EMV, then who will bear the loss? Payment association will decide. If both the banks are EMV complaints, this will never happen.

Therefore, to prevent the cards being counterfeit, the customers, merchants, banks and payment associations need to undertake some precautions described in this module under the heading "5.7. Card Fraud Prevention Strategies".

5. Debit Card, Credit Card, Card technologies and Card Frauds

Today it is already impossible to imagine modern bank operations, commercial transactions and other payments without using a **card**. Cards due to reliability, universality and convenience, which won the deserved recognition all over the world, have received a wide circulation. So, now, the Visa cards holders' number makes more than 300 million. Also, about 300 million clients are totaled by other largest payment system presented as MasterCard, American Express (AmEx), Diners Club (DC), JCB, and numerous national, regional and local (inter- and mono bank) one-currency systems.

Approximately 90% of adults hold one or more cards in UK and USA.

In the sphere of financial services in Bangladesh during the last few years, the new kind of payment means like "Q-Cash" is used on the cards base (magnetic and chips) in addition to the proprietary cards of Dutch-Bangla Bank (Nexus Card), and branded cards from VISA and MasterCard issued by different banks.

5.1. Card types

There are many varieties of cards. Most popular cards are listed below:

a) Credit Cards

Credit cards are issued once the customer is assessed for the credit limit and has entered into an agreement with the card issuing bank. The card permits the customer to buy goods and services straight away up to an agreed limit amount and pay in full within a set grace period (40-50 days from the billing date) without paying any interest. Most Credit card issuing banks have a set minimum payment which is usually Tk.500/- or 5-10% whichever is greater. The

customer can choose to pay minimum amount or higher or full amount within the grace period. If the customer pay partial, interest will then be charged on the outstanding debt each month.

A monthly statement is sent to the customer showing his account details, what he spent, where, on what date and how much is owed. The full amount can be re-paid which may mean the customer would avoid any interest charges or if he chooses to repay a lesser amount he will incur interest charges. A credit card is usually be used in POS terminals, however can be used in ATM to withdraw money but interest may be charged on cash withdrawal amount from the day the money is withdrawn. Some credit card issuing banks offer Signature, World, Platinum, Titanium, gold or silver credit cards. All the cards provide credit facilities but each type of card has different conditions and benefits.

b) Debit Cards

These cards are a substitute for using cash or writing a cheque. The money is taken directly from the customer's bank account. The card can be used in ATM machines allowing them to withdraw cash from their own bank account and it is also used in POS terminals to pay for goods & services.

c) Pre-Paid Cards

These are cards that the customer load with cash and they then use the card as an alternative to cash. These are generally used for small purchases or to buy on the Internet.

d) ATM Cards

These are also known as a cash card, cash dispenser card or cash machine card. This card is used in an ATM for cash withdrawals and other banking services.

5.2. Terminology for Card transactions at ATM and POS terminals

5.2.1. Issuer and Acquirer

The Bank or an organization which issue card is called issuer. If you are having a credit / debit card of DBBL, your issuing bank is DBBL.

The Banks or payment organizations which install ATM or POS terminals at merchant locations are called Acquirer. If you are using a card of DBBL at an ATM of BRAC Bank, the acquiring Bank, in this case, will be BRAC Bank. If you have asked for an amount of Tk.10,000 at the ATM, but ATM dispenses less money whereas your account has been debited in full, you have to log complain with your issuing bank, not with the acquiring bank.

5.2.2. On-us transaction

In a transaction, if the issuing and acquiring banks are same, then the transaction is called ON-US transaction. For example if a customer of Bank-A, makes a transaction at the ATM / POS of the same bank (Bank-A), then the transaction is termed as on-us transaction.

5.2.3. Off-us or Not on-us transaction

If customer of another bank makes a transaction at the ATM / POS of our Bank, the transaction is called off-us or not on-us. For example if a customer of Bank-B makes a transaction at the ATM / POS of Bank-A, then the transaction is termed as off-us or not on-us at Bank-A. However this transaction will be termed as remote on-us at Bank-B.

5.2.4. Remote on-us transaction

If customer of our bank makes a transaction at the ATM / POS of their Bank, the transaction is called remote on-us at our bank. For example if a customer of Bank-A makes a transaction at the ATM / POS of Bank-B, then the transaction is termed as remote on-us at Bank-A. However this transaction will be termed as off-us or not on-us at Bank-B.

5.2.5. Interchange fee:

If a customer of Bank-A makes a transaction at the ATM of Bank-B, then Bank-A will pay a charge to Bank-B. Bank-A will realize such charges (normally more than this amount) from the customers and pass on the set amount to Bank-B.

On the other hand, if a customer of Bank-A makes a transaction at the POS of Bank-B, then Bank-B will pay a charge to Bank-A. The Bank-B will realize this charge from the sale proceeds of the POS merchant, which is called merchant commission.

The above charges payable by one bank to another bank is called interchange fee. The interchange fee is fixed by international payment associations like MasterCard, Visa, Dinar Club, Discover, JCB and may vary for local and international cards, EMV and non-EMV cards or card types (Signature, Platinum or Gold card), or transaction types (Utility bills or merchant payment). The interchange fee may also be determined by the Central Bank.

5.2.6. Merchant Commission:

Bank provides POS terminals to the merchants (shops, hotels etc) free of cost. Bank also supplies necessary papers for POS terminal and performs regular maintenances. In lieu, bank realizes a commission from the sale proceeds of the merchant. This commission is called merchant commission. The merchant commission varies from merchant to merchant (based on total sale volume of the merchant), which ranges from 1.50% – 3.00 % for branded card, and from 1.00% – 2.00% from proprietary cards.

5.2.7. EMV and Chip Card

The conventional cards contain magnetic strip at the back of the card which stores customer and card related information. Retrieval of information from a magnetic strip is easy. When the card is handed over to the merchant for transaction or used in the ATM, hackers can easily copy the information inside the magnetic strip and produce a duplicate card. Using this duplicate card, they perform fake transactions at the POS or ATM (if PIN can also be collected, which is not stored in the meg-strip). This type of fraudulent activities has been increasing day by day. To protect this, Europay, MasterCard and Visa jointly devised a security mechanism called EMV. EMV stands for Europay-MasterCard-Visa. In an EMV card the information are stored in the computer chip using some computer algorithm which is very difficult to copy and retrieve. A normal chip card and an EMV chip card use computer chip, but the EMV card, in addition, has some computer logic prescribed and certified by Europay, MasterCard and Visa. Thus EMV card is most secured card in the world. Europay, a payment association, has been purchased by MasterCard.

Figure: An EMV Card

5.2.8. Liability Shifting

EMV has announced a rule called Liability Shifting, which said that if a fraud is occurred, the non-EMV party will always be responsible for the fraud, thus non-EMV party has be pay the fraud money to the EMV party. Thus if a customer uses an EMV card anywhere in the world, and if fraud occurs in any non-EMV ATM or POS terminals using his card number, the customer and his issuer are always safe.

If the ATM and POS are EMV certified, the MasterCard and Visa's EMV technology guarantees that the fake card will not be accepted at these terminals as these terminals will never read the meg-strip part of an EMV card. If the ATM and POS terminals are not EMV certified, they will not be able to read the chip, rather will read the meg-strip part of an EMV card.

5.2.9. Charge Back

If a fraud occurs using a card of Bank-A at the POS/ATM terminal of Bank-B, Bank-A's customer's bank account or credit card account has been debited. Thus when the customer will receive his statement of account, he will find that some transactions are reflected in his

statement which are not made by himself. He will, then, report this to his issuer (bank). The issuer will analyze the transaction and if found that as per the rule of the payment association they have the right to get the money back from the acquiring bank, they will bring the money back to their nostro account via the payment association. This process of bringing the money back is called Charge Back.

5.3. International Payment Associations

Plastic Money can be classified by payment associations / systems or card associations. The most famous payment associations / systems are MasterCard, Visa, Amex, JBC, Dinar Club, Discover and Union Pay of China. One card can be supported and serviced by only one payment system.

Some payment associations / systems can emit only cards of some types. For example American Express and Diners Club emit credit cards only, and others may emit only debit cards. World famous leaders such as VISA and MasterCard emit and support both types of cards.

Credit cards of different systems are divided into classes. VISA has four main classes: Classic, Gold, Platinum and Signature. MasterCard has classes: Standard, Gold, Titanium and World.

5.3.1. MasterCard

The MasterCard story begins in 1966 when a group of banks created a member-owned association that later became MasterCard. In 1968 the company extended its presence to Mexico, Japan and Europe, marking the start of its commitment to becoming the leading global payments network. Through the 1980s, MasterCard continued to build on this promise, bringing the advantages of electronic payments to new regions and markets around the globe.

MasterCard integrated with Europay International in 2002, establishing a unified global corporate structure and also becoming a private share corporation.

Global Headquarters
Purchase, New York

Employees
Approximately 5100 (located in offices around the world) as of the year-2010.

Global Regions
MasterCard is organized geographically into the following regions: Asia Pacific Middle East Africa; Canada; Europe; Latin America; and the United States.

MasterCard Worldwide Brands

MasterCard is one of the most widely recognized **credit** and **debit** card brands in the world, representing instant buying power, immediate deposit access convenience, security worldwide, and flexible payment options.

Maestro is one of the most widely recognized global **debit** card. It is the only online, PIN-based debit brand that can be used to make purchases and get cash at ATMs worldwide.

Cirrus is the brand name that stands for the global MasterCard/Cirrus ATM Network, among the largest ATM networks in the world. The Cirrus brand represents immediate deposit account access convenience at more than one million cash machine locations worldwide.

Figure: A Credit Card (MasterCard) and a Debit Card (Maestro) of MasterCard

Membership:

Through the thousands of financial institutions that are MasterCard's customers, the company markets a strong portfolio of brands and products worldwide, including MasterCard, Maestro, Cirrus, MasterCard Debit and MasterCard *PayPass*.

MasterCard provide two types of membership – Principal Member and Associate Member. Principal Member is a direct member and it has direct connectivity with MasterCard network using a MIP (MasterCard Interface Point) which needs to be established at the Data Center of the Member Bank. An Associate Member does not need to setup MIP and thus it routes all the transaction through a Principal Member to which it is an Associate Member. The Associate Member also needs to pay less membership fee and charges.

5.3.2. VISA

Visa is a global payments technology company that connects consumers, businesses, banks and governments in more than 200 countries and territories worldwide. Visa Inc.'s headquarters are in San Francisco. Visa has approximately 5,500 employees around the world as in the year-2010. They operate three data centers on two continents. Visa Europe is a separate

membership entity that is an exclusive licensee of Visa Inc.'s trademarks and technology in the European region.

Today, Visa network spans:

- 15,900 financial institution customers
- 1.7 million ATMs[2] *(as of March 31, 2010)*
- 200 countries and territories
- 1.8 billion Visa cards *(as of March 31, 2010)*

Visa Products:

Credit Products:

Visa offers various VISA credit cards such as Visa Platinum, Visa Signature and Visa Infinite. All Visa credit cards come with standard benefits and features, including Auto Rental Collision Damage Waiver, Emergency Card Replacement and Zero Liability protection that safeguard cardholders against unauthorized purchases.

Debit Products:

Visa debit cards such as Visa Electron and Visa Debit are safer than carrying cash, more convenient than writing cheque. Visa debit cards offer security protections that help prevent, detect and resolve fraud, including continuous fraud monitoring and coverage by Visa's Zero Liability policy, which protects cardholders from unauthorized charges.

Pre-paid products

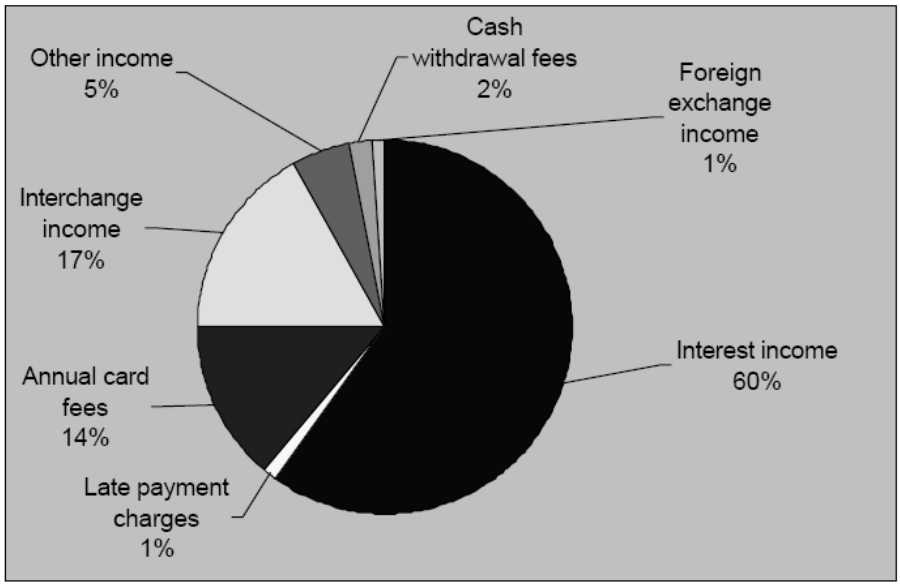
Visa provides a wide range of Visa prepaid cards and services through retailers, financial institution branch offices, employers and government agencies, including:

- Visa reloadable prepaid cards
- Visa Gift cards
- Visa TravelMoney cards
- Visa Healthcare cards
- Visa Payroll cards
- Visa Incentive cards
- Visa Government Disbursement cards
- Visa ReadyLink, Visa's prepaid reload network

Figure: A Credit Card (VISA) and a Debit Card (VISA Electron) of Visa

5.4. Income from Credit Card Business:

There is a variety of incomes for the issuer and acquirer such as interest income, annual card fee, interchange income, cash withdrawal fee, late payment charges, foreign exchange income etc., as may be seen from the following chart:



Source: Visa International (2000).

5.4.1. Sources of income from Debit Card issuing (payable by cardholder):

1. Card issuance fee
2. Annual / Renewal fee
3. Card replacement fee

4. PIN re-issue fee
5. As issuer of debit card, the bank's low cost deposit increases significantly which indirectly contribute to generation of income for the bank.

5.4.2. Sources of income from Credit Card issuing (payable by cardholder):

1. Card issuance fee
2. Annual / Renewal fee
3. Card replacement fee
4. PIN re-issue fee
5. Interest on Outstanding debit balance
6. Late payment fee

5.4.3. Sources of income from ATM acquiring (Payable by cardholder / issuing bank)

1. Interchange fee (if the cardholder of another bank is using the ATM)
2. Cash advance fee (If a credit card holder withdraw money from ATM)
3. Consumer paper fee (fee for taking paper slip)
4. Video retrieval fee (retrieval of CCTV video as per customer's demand)

5.4.4. Sources of income from POS acquiring (Payable by Merchant / Cardholder)

1. 1.50% – 3.00% commission on the sale value (payable by Merchant)
2. Exchange earning in case of foreign transactions (realizable from Cardholder)

5.5. Card Technologies

5.5.1. Plastic

Plastic card is a plate with standard dimensions (85.6 mm. x 53.9 mm. x 0.76 mm.) produced from special, mechanic- and thermo-resistant type of plastic used to store information.

5.5.2. Magnetic Strip and Micro Chip

As electronic data media, the cards are divided into magnetic strip cards and integrated chip (microprocessor) cards. The first ones are called magnetic cards, the other ones are smart cards, or chip cards.

Cards with a magnetic strip are the most widespread today – circulation is over two billions. The magnetic strip settles down on the back side of a card and, according to standard ISO 7811, will consist of three tracks. First two of them are intended for storage of the identification data, and on a third it is possible to write down the information (for example, the current value of a limit of a debit card). However because of low reliability of repeated process of recording / reading, recording on a magnetic strip, as a rule, is not practiced, and such cards are used only

in a mode of reading of the information. However such type of cards is rather vulnerable for swindle. In the USA in 1992 the total damage from frauds with credit cards with a magnetic strip has exceeded one billion dollars.

On a magnetic strip card the following data is provided:

a) on a card's face one can find:

- Owner's name
- Card number
- Card's validity
- A logo of a card's issuing bank
- Payment system logo

Some cards have holograms for extra protection.

b) on the opposite side there are:

- A place for an owner's signature
- Magnetic stripe
- Owner's photo (in some cases)
- Logos of ATM networks where the owner can perform operations with the card

Card number consists of 16 digits:

- The first six digits- a code of an Issuing Bank
- The following nine numbers – card's bank number (card account number)
- The last one - control digit

In smarts cards a data carrier is the microprocessor / micro-chip - the memory size of which can store from 32 bytes up to 16 kilobyte. This memory supposes unitary recording and repeated reading, or admitting both repeated reading, and repeated recording.

Smart cards were invented in the early 1970s. In the mid-1980s, French banks began widespread use of the technology as retail transaction debit cards.

The microprocessor allows to take certain actions on the data stored in the card via the card's operating system with multiple functions for memory and service control and security measures.

The microchip embedded in smart cards can be a simple memory-only device (also called IC cards for integrated circuit) or a complex read/write microprocessor (also called a central processing unit or CPU). Now-a-day normally Chip is available with eight kilobytes storage capacity, which can hold 1,600 words of text or a digital snapshot of a fingerprint, palm print or retinal scan. It is predicted that 16-kilobyte chips will be available soon and that a 64-kilobyte chip will be produced sometime in the next decade - the sky is the limit.

Encryption makes access control applications more secure. One can set up his reader so that it requires a cryptogram to be correctly passed between the card and the reader - like a challenge and response. The reader will challenge the card with a number and the card has to encrypt it and send it back to the reader. The reader checks the response to see if it is correct. Only an authentic card will know how to encrypt it because it is the only one that knows the particular encryption keys that have been set up for that application.

5.5.3. Personalization of bank cards

Depending on the type and purpose of plastic cards, one can choose various types of personalization:

- Encoding of chip-module
- Recording on magnetic strip (HiCo, LoCo)
- Imprinting of unique numbers (pin, login) covered with scratch-strip by means of thermo-printer or bubble jet
- Embossing with tipping
- Imprinting of bar code

Encoding – Recording of information on the magnetic strip or micro chip.

LoCo – Low-coefficient magnetic strip (300 oersted).

HiCo – High-coefficient magnetic strip (noiseproof, up to 4,000 oersted) with high resistance to magnetic fields, i.e. information that is protected on a magnetic strip is difficult to delete using a magnetic field.

Embossing – A method of mechanically pressing information comprising from letters and digits onto a plastic card; allows significantly faster payment by imprinting a slip on it.

Tipping – Covering embossed symbols with a painted film to stand out from the background images of a plastic card; most often uses gold, silver or other metallic colors; The needed brightness is achieved by adding black or white paint.

Signature strip – A special strip on a card for inputting a signature or other information; can be with or without captions that prevent the signature to be rubbed off.

Hologram – A holographic sticker that is pressed onto a card under high temperature; functions as an additional level of protection from creating imitation cards; comes in two types, 2D and 3D.

5.6. Card Fraud

The `pickpocket' method to steal a card and using fraudulently in a POS terminals was used back in the 1980s. Now they are deploying state-of-the-art equipment in their scams. In this digital age, credit card fraudsters use "skimmer" machines to read and duplicate the personal data encrypted in the magnetic strip of a card. They do not even have to get hold of the card anymore, as they can tap directly into telecommunication lines used for credit card transactions and intercept card data. Meanwhile, as using credit cards for online transactions becomes more common, "phishing" techniques have developed to steal card data.

Plastic card fraud was one of the fastest growing crimes in the UK in the late 1980s and early 1990s. Losses more than doubled over the period reaching just over £165 million in 1991. The major banks and building societies agreed that collective action was necessary to stem the losses and in September 1990 they formed the Plastic Fraud Prevention Forum (PFPF).

The immediate measures introduced by the industry (banks, payment systems etc.) in the early 1990s focused on those areas where most fraud was committed, i.e. on lost/stolen cards being used over the counter in shops and stores. Initiatives included:

- The introduction of lower floor limits (the amount above which a retailer needs to seek authorization from the card issuer) particularly in fraud-prone retail sectors, so that more transactions had to be referred for authorization.

- Use of 'hot card files' - lists of cards reported lost or stolen - broadcast electronically to the point-of-sale (POS) terminals so that retailers could check a card automatically.

- Delivering cards to the customer using more secure forms of delivery.

- Enhancement of security features within the card. These include the hologram and information enhancements to the magnetic stripe.

- Working with retailers to encourage co-operation with the introduction of POS initiatives.

- Dialogue with police of all levels.

- Promoting practical advice for cardholders and good practice for retailers through campaign.

The success of the above initiatives leads the fraudsters to targeting new areas such as:

5.6.1. Counterfeit

Counterfeit is the fastest growing fraud-type. Cards used to perpetrate fraud are generally lost or stolen cards which could be used intact or altered by re-embossing and re-encoding, or counterfeit cards that are entirely new. In order to counterfeit a card it is necessary to know the

details of a current valid cardholder -- hence the desire of offenders to obtain legitimate credit card details from sources such as the Internet (a method which is being used increasingly by offenders throughout the world). Blank, white plastic cards are then embossed with stolen numbers, the magnetic stripe is encoded with matching numbers, and the signature panel on the card installed. Identifying logos and color printing are added to mimic a real card.

Sometimes information on the card's magnetic strip is obtained by "card skimming". This is when a legitimate card is obtained for a few seconds to enable it to be passed over a magnetic tape reader so that a counterfeit copy may be made.

Another technique is "buffering", which involves modifying the information stored in the magnetic strip of the card or obtaining security codes electronically.

Although magnetic stripe cards are relatively easy to forge, smart cards are more difficult to counterfeit, but there are claims that they are not absolutely tamper-proof.

To protect against it, chip cards built to an internationally-agreed standard are being introduced. Retailers are also being trained in techniques for spotting counterfeit cards.

5.6.2. Application Fraud

Frauds relating to the issue of cards may be perpetrated in one of two ways:

First, so-called "true name fraud" occurs when an offender obtains the personal details of a real person and uses them to acquire credit cards in that name. The offender then uses the cards to purchase goods for which the liability passes to the legitimate cardholder.

The **second** type of fraud involves the use of false identification details, which are used to obtain a legitimate card in a false name by individuals who later default on payment and abscond.

5.6.3. PIN Fraud

Other vulnerabilities arise out of the way that the individual making use of the card authenticates his or her identity when using the card. This is mainly a problem with debit cards used in electronic card reading machines, which can verify the identity of cardholders by requiring them to enter a PIN or password. In order to enhance the security of the system, the user's PIN is encrypted before it travels through the network, thus making it difficult for the PIN to be discovered by hacking into the network.

A more substantial security risk arises from the manner in which the PIN is communicated to the cardholder, recorded and remembered by the cardholder, and used by the cardholder at a terminal during a transaction. Although cardholders are clearly warned of the dangers associated with disclosing their PIN, writing it on the card, or keeping it in the same place as the

card, a considerable proportion of cardholders refuse to heed such advice, thereby placing themselves at risk of loss - for which they will be personally responsible.

5.6.4. Card Not Present

The rise in sales transactions through internet payment gateway has led to significant growth in fraud where the card is not present. At present, most commercial transactions which take place on the Internet are undertaken by customers purchasing goods and services by disclosing their credit card details. It has been estimated that transactions valued at approximately $A640 million took place on the Internet in 1995, and by the end of 2005 global online commerce is expected to reach between $A97 billion and $A238 billion.

Credit card information is illegally obtained either by hacking into databases of account numbers which are held by Internet service providers, or by intercepting account details which travel in unencrypted form. There are also many online scams perpetrated by customers who make use of false credit card details, as well as merchants who fail to honor online agreements.

The banking industry in UK implemented an automated system in 2001 to enable merchants to verify the billing addresses of cardholders and cross-check coded digits on cards to make these types of transaction more secure.

5.7. Card Fraud Prevention Strategies

There are four primary strategies which can be used to prevent plastic card fraud.

5.7.1. Action by Card Issuers

Card issuers can adopt a wide variety of strategies to reduce the risk of plastic card fraud. The most pressing need is for financial institutions not to issue cards to individuals unless they are satisfied of their identity.

Various procedures could also be adopted to ensure that plastic cards are not stolen and that cards and PINs are communicated securely to customers. Banks could also assist merchants by notifying them promptly of stolen cards and PINs.

Cards could also be required to display the holder's photograph.

One of the main strategies used to prevent EFTPOS fraud has been simply to lower floor limits (the transaction value at which authorization is required from banks before the card can be accepted).

Finally, various transaction monitoring strategies have been suggested to minimize losses through smart card fraud by quickly identifying fraudulent transactions and limiting the maximum value of transactions.

5.7.2. Action by Merchants

Frauds involving merchants constitute a large problem for financial institutions as merchants or their employees are ideally placed to handle the customer's card, to permit access to computer networks and to alter transaction details.

Finally, merchants should examine any suspicious behaviour and appearance of customers. This might involve customers selecting purchases rapidly; being dressed inconsistently with the nature of the purchases selected; customers who split purchases between various slips in an attempt to forestall authorization calls to issuers; customers who make multiple purchases all under the floor limit; and customers who buy many of the same items but in different colors and sizes.

Unfortunately, it is often not possible for merchants to use all of these techniques through fear of deterring potential customers.

5.7.3. Action by Cardholders

Protection of one's card, PIN or password is the primary crime prevention strategy which card holders need to take. Although consumers are advised not to disclose their PIN, keep it with their card, or write it on the card, studies have revealed that between 20 and 70 per cent of people fail to adhere to such advice.

5.7.4. Technological Solutions

A wide range of technological solutions have also been devised in order to reduce the security risks associated with plastic card payment systems.

5.7.4.1. Protections against Card Counterfeiting

Various strategies have been devised to enhance the security of plastic cards and to make them more difficult to alter or counterfeit. These include the use of micro chip, holograms, embossed characters, tamper evident signature panels, magnetic stripes with improved card validation technologies, and indent printing.

5.7.4.2. Card Restrictions

As an alternative to target hardening, the risk of large-scale fraud through the use of plastic cards could be reduced by placing limits on the size of card-based transactions or the amounts of money that may be stored on plastic cards. There could also be a limit on the life of the cards.

5.7.4.3. Fraud Detection Software

Software has also been devised which is able to analyze plastic cardholder spending patterns in order to alert individuals to the presence of unauthorized transactions. Merchant deposit monitoring techniques also exist to uncover claiming patterns of corrupt merchants. One software package called PRISM (Proactive Fraud Risk Management) is used to detect credit card fraud carried out through the use of lost cards, stolen cards, counterfeit cards, fraudulent applications, cards never received, mail order, phone order and catalogue sales and merchant fraud. The cost is between $384,000 and $1.92 million depending on system requirements and configuration. While initial installation costs may be high, the benefits obtained through the prevention and detection of fraud makes the use of such systems worthwhile for large organizations.

5.7.4.4. Improved Cryptography

Finally, cryptography, which is the mainstay of electronic banking security systems, could be improved to protect data transmissions over the net. This is currently being explored to secure online electronic cash systems by joint ventures such as MasterCard and Visa International's Secure Electronic Transaction Protocol, which uses public key encryption to protect data from being compromised, and is expected to be fully operational shortly.

5.7.4.5. EMV

a) What is EMV?

EMV is standard for **Smart Card** Debit / Credit. EMV was jointly developed by Europay, MasterCard and Visa. Recently JCB and Amex have joined EMV as well. Latest version is EMV 2004.

A Smart Card is a computer chip and contains the following:

- Memory
- Storage Space which stores Card ID, Owners ID, PIN, Authorization Levels, Cash balance, Credit Limit
- An Operating System such as Native OS, MULTOS or JavaCard
- Application Programs – standard routines

EMV has incorporated mandatory and optional steps defined by EMVCo such as:

- Secure Card Authentication Method (CAM) through Static Data Authentication (SDA)
- Dynamic Data Authentication (DDA)
- Combined Data Authentication (CDA)
- Secure Cardholder Verification Method (CVM)
- Enhanced Risk Management

- Contains certain defined Application Programming Interfaces (API's) and certain physical and electrical standards

b) What is EMVCo?

EMVCo is a company formed by Europay International, MasterCard International and Visas International in February, 1999. In 2002, acquisition of Europay International was made by MasterCard International. In 2004 and 2009, JCB and Amex joined EMVCo respectively. Currently Amex, JCB, MasterCard & Visa each have 25% share.

c) Benefits of EMV:

- Prevent Counterfeit card
- Secure transaction off-line, no need to go all transaction to on-line. Saves online cost.
- Possibility to lose amount in chip-liability shift
- Easy to implement various programs such as contactless MasterCard PayPass.
- Higher revenue from a non-EMV issuer and Acquirer.

d) Why Banks should move to EMV?

- Interoperability
  - Of card acceptance, security and payment functions
  - Liability shift

- Enhanced security
  - Cryptography, offline risk management with a common decision being taken between card and terminal
  - Protection against counterfeit fraud, lost or stolen (through offline PIN)

- Better Control
  - Sophisticated authorization decisions off-line/forced on-line
  - Issuer controlling the risk
  - Customer centric decisions at the terminal, control managed within the application on the chip

- Operational Savings
  - More off-line processing, fewer chargebacks, longer card life

- Issuer can update the card at the terminal:
  - Change parameters via "scripting"
  - Add/activate new applications – like card level loyalty.

e) What is the risk of counterfeit in Meg-strip card?

i) The card can be copied with a $50 USD small device.
ii) The track information is not encrypted and is very easy to personalize cards with copies data.
iii) Copied Data can be altered very easily before personalizing counterfeit card.

f) How does EMV protect Counterfeit fraud?

i) Copying chip data is not easy (may be possible with billion dollar investment)

i) In DDA card, copying chip data and making counterfeit card is not enough as this type of card generates dynamic key by processor inside the card which is unique for each DDA card which we call ICC key. Card data is signed by this ICC private key which can't be decrypted without this particular card ICC public key.

Note: DDA stands for Dynamic Data Authentication which:

1. provides authenticity and integrity of ICC and terminal dynamic application data (signed by ICC private key).

2. Allows detection of unauthorized alteration of ICC data after the card has been personalized.

3. Prevents replay attacks and ICC counterfeiting.

iii) The card information in a DDA card is kept encrypted three times by a) Card Key (also called ICC key, this is card specific key), b) Issuer private Key (RSA key generated by Issuer host), c) CA signed IPK (Issuer public key encrypted by EMVCO CA private key).

iv) The public key can decrypt the private key and all the terminals have the EMVCO CA public key.

v) The card can decide itself what actions to take for a particular transaction (depends on the txn amount, txn frequency, txn type) according to the IAC (Issuer Action Code) in the Chip card set by issuer at the time of personalization. The response may be approve offline, decline off-line or go on-line.

vi) For On-line transactions, after getting the card data in the above decryption processed, the card data is further encrypted by UDK (unique derivative key, this is TDES key) and generates ARQC (authorization request key). This UDK is generated from MDK (master derivative key) at the time of personalization. This MDK is shared also stored in the Issuer Host. When an ARQC for a transaction comes on-line to Issuer host, the host decrypts the data with that UDK (as the host has the MDK), if it finds the card data ok and other validations are done at the issuer host, the Issuer host sends back an ARPC

(authorization response code) which is signed by UDK. As the card also has the UDK (earlier mentioned, card contains the UDK at the time of personalization), it can decrypts ARPC and can see what Issuer Host advised.

g) What are main contents of a meg-strip card and chip card?

Meg-strip card contains Track1, Track2 data which records Card name, Card Number, Expiry date, CVV, PVV etc.

Whereas chip card contains:

i) All the information of Meg-strip data in specific fields

ii) Card data under ICC private key

iii) ICC public key under Issuer private key

iv) Issuer Public Key CA private key

v) UDK (for generating ARQC for Online)

vi) UDK(Mac), UDK(Enc) (for Issuer Script Update)—Same UDK values are kept in the card and Issuer host, thus It validated & update the scripts sent by issuer & vice versa.

6. Internet Banking

Internet banking is also known as i-banking or on-line banking. Internet banking is a system which the customers can access from his home, office or anywhere in the world through internet. To avail this service, the customer needs to get an user ID and password from his bank and he need to have access to a computer with internet connection.

6.1. Internet Banking Password

When the customer accesses the i-Banking for the first time, the system will ask for changing his password. The customer must change the password as per the password policy of the bank. For example a bank may have adopted the following password policy:

- Length must be min. 6 - max. 12 characters
- User ID is not allowed as a part of the password
- Password should have at least 1 upper case, at least 1 lower case, 1 numeric digit and no symbolic characters
- Number of identical characters: 2

The following is the valid password: Joyful7, raiN567

The following are not valid passwords: Joy7, rain567, rain666, aaAmin2

6.2. Internet Banking functions

The customers can perform almost all types of banking activities through i-Banking except cash transactions.

Account Summary

The customer will be able to view the list of Current, Savings, Term Deposit and retail loan accounts held and the Current Balances in each account in the account currency. An indicative valuation of the account balances can be performed in the customer's preferred currency

Account Details

The customer can choose a particular account (Savings, Checking account, Term Deposit or Loan account) and see the account details such as date of opening, date of maturity, outstanding balance, interest accrued, interest paid, limit amount etc.

Account Activity

The customer can see transaction activity in a given account for a range of dates specified by the customer.

Transfer Funds

The customer can transfer funds from his one account to his another account with the Bank.

Open Term Deposit (TD)

The customer can open a Term Deposit by transferring funds from one of his current or savings accounts with the Bank.

Modify Term Deposit

The customer can modify the maturity and interest instruction details of the existing term deposit accounts.

Close Term Deposit

The customer can close a TD account prematurely in part or in full. He will be shown the penalty applicable as per the product definition.

Loans Repayment

The customer can make payment of the Loan instalment or any amount by specifying the amount. The amount will be transferred from his deposit account.

Early and Final Settlement

The customer can make an early payment of the entire loan amount due. The amount will be transferred from his deposit account.

Standing Instructions – The customer can setup standing instructions for transferring a fixed amount of funds from his deposit account to another deposit (self or third party) or loan account in the bank in a fixed date of every week / month / quarter / year. He can specify the start date and the final date for execution of the standing instruction.

The users can set-up multiple instructions for each account and define the priority in which they can be executed. The instructions can be setup for one–time transfer or for recurring transfers at a pre-defined frequency.

Payee maintenance – The customer can set up templates for use in 'Third party Funds Transfer' mentioning account number and other details of the 'Third Party'. The 'Third Party' means an individual who has account with the same bank. However an educational institute or utility company is not a 'Third Party'. To be effective and available in the list during the "Third Party Transfers", such entries need to be approved (authorized) by a bank officer.

Third Party Transfers - The customer can transfer funds from one of his accounts to another 'Third Party' account within the bank. The 'Third Party' account must be pre-recorded in the system using 'Payee Maintenance' and authorized by a Bank Officer for making this available in the list.

Statement Request

The customer can make a request for account statement for a required period. The bank will manually service this request.

Cheque Book Request

The customer can make a request for a cheque book for an account choosing the number of leaves desired from the set that the Bank offers.

Stop Cheque Request

The customer can choose an Account and enter the cheque number/range of cheque numbers for which the cheque encashment should be stopped. He can also specify the reason for stopping the encashment.

Cheque Status Inquiry

The customer can choose an Account and enter the cheque number for which the status should be viewed. In case the cheque is returned or stopped, the reason for rejection will also be shown.

FX Rates Inquiry

The customer can query on the FX rates that the Bank offers using this function. The rates displayed are the TT, cash and DD rates.

Interest Rates Inquiry

The customer can query on the interest rates offered on Savings & Term Deposit Products offered by the Bank.

Change Password

The customer can voluntarily change the Internet password using this function. In addition the user is forced to change the password by the system at first Logon and defined intervals. In both cases the password needs to conform to the policy defined by the bank.

Letter of Credit

Letter of Credit – Initiate

The customer (company) can choose to initiate LC. One officer of the company will fill-in the LC screens from his office. Another higher level officer will authorize the LC and submits to the Bank. The relevant branch officer will examine the entries and verifies with the documents or scanned copies of the LC documents, and authorize. After authorization by the bank, necessary accounting entries will be passed in to the Core Banking System and SWIFT message will be passed.

The data entry (by an officer of the company) in the LC screen will comprise of multiple screens, which will provide Save and Submit options. The Save option will facilitate saving of partial or incomplete data entered in each Screen. Data will be finally submitted when the Submit option is invoked. Validations of the data entered in all the screens will be done and incase of an error(s) it will be displayed to the user.

A verification and confirmation (by higher level officer of the company) screens will be displayed at the completion of the initiation of a LC and will be a Single Screen. Audit Information at the bottom of each screen will be displayed, the contents of which will be the Initiator Name & Date & Authorizer Name and date corresponding to it.

Letter of Credit – Modify

The customer can modify the LC under certain scenario such as:

The transaction to be modified has to be initiated by the same user.

In addition the transaction to be modified has to be either in an Incomplete State or is Unauthorized or rejected by the authorizer.

Audit Information at the bottom of each screen will be displayed the contents of which will be the Initiator Name & Date & Authorizer Name and date corresponding to it.

Letter of Credit – Authorize

The Authorizer can only authorize those LC Transactions for which he has rights. Rights will be based on the Initiator and the Transaction Authorization Limit. Once the transaction is authorized it will be directly sent to core banking system.

Authorizer can also reject a LC. A facility to specify the Reason for rejection is provided. Audit Information at the bottom of each screen will be displayed, the contents of which will be the Initiator Name & Date & Authorizer Name and date corresponding to it.

6.3. Fraud in Internet Banking:

If we look at the functionalities covered under the Internet banking system as mentioned above, we can see that if a fraudster can know the ID and password of a customer, he can easily get access to the system and do the following:

1. Can get the number, outstanding balance and transaction history of all the accounts maintained by the customer in the bank (**stealing confidential information**)
2. Can transfer the money from customer's one account to the customer's another account or to an utility company's account (**harassment**)
3. Can transfer the money from customer's account to the fraudster's account and withdraw money from ATM (**real fraud**)

To protect the customers from above frauds, Banks need to protect stealing his password while travelling from customer's computer to the Bank's server or from phishing attract. Banks may also introduce a mandatory 2-factor authentication for a 3rd party transfer and LC transmission.

These protection measures are described below in brief.

a) Capture of Password during transmission to the bank server

While the Password is travelling through internet from customer's computer to the Bank's server, a Fraudster can easily capture it and use the information to enter into the internet banking system. To protect the PIN from capturing during travel, the bank' system must be capable to encrypt the PIN and bring into the server and decrypt them before further processing. If a Fraudster capture encrypted information on the way, it is not possible for him to decrypt and find the real information. As such the PIN on the way is safe.

b) Phishing

Phishing is collection of user PIN by presenting a fake web-site address to the user. For example, let us consider that the website address of a Bank is www.abc-bank.com. Hacker will develop a fake website exactly similar to the website of the Bank, but with a different address such as www.abe-bank.com and place in the internet. Now if a user searches for the "ABC" bank in the Google, address of this fake website will be shown in the search result. Now if the user clicks on this link, he will go to the fake website. If he does not look at the website address carefully or the address is not known to him, he will insert his ID and Password into the fake web-page. The hacker will record all such attempts made by different users and collect ID and Passwords.

The false website address may also be sent to various users through email where in the name of a bank, the customer will be requested to enter into his i-Banking system and check something. The users, who are not aware of phishing attracts, may try to login into the false website using his ID and Password. All such information will be captures into the hacker's database.

The hacker can now use the collected ID and Password to enter into the i-Banking System and do fraudulent activities.

It may not be possible for customers to know the exact website address of the Bank.

It is therefore devised that the website of a bank which offers i-Banking may be certified by a certifying authority such as VeriSign. The page of the bank which collects customer's ID and Password will display seal of the certifying authority. If a

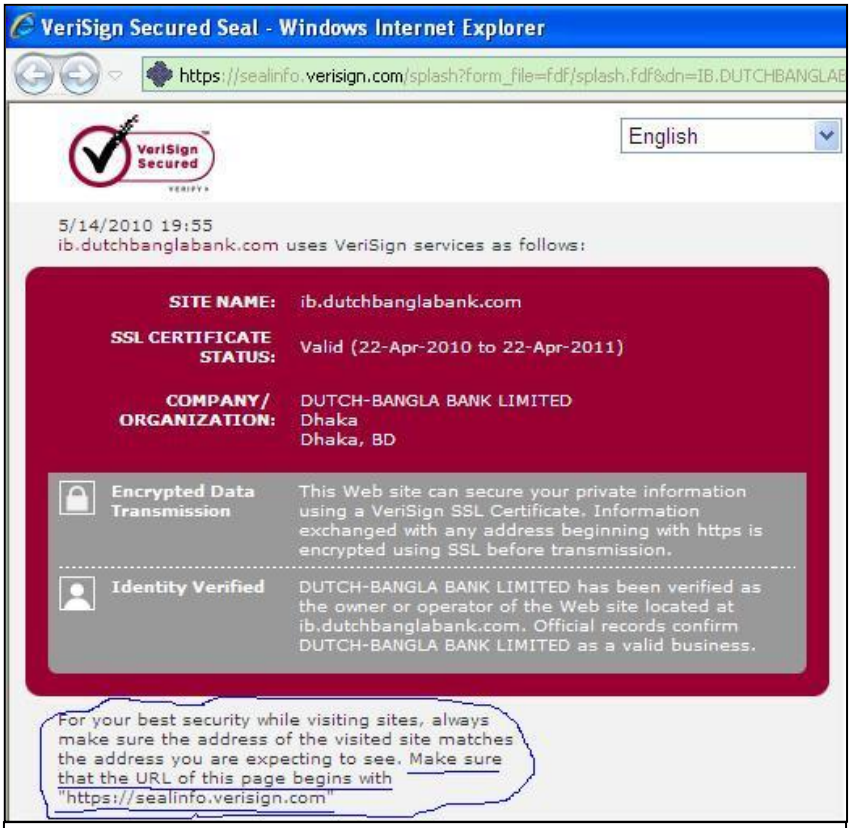


Figure: The address of the VeriSign website should be known to the users

customer clicks on the seal, the website of the certifying authority will appears. All the customers must know the web address of the established certifying authority and thus should be able to verify its correctness. If the website address of the certifying authority is correct, the website page of the bank is also correct. As such the customer can insert the ID and Password safely into this webpage.

c) Repudiation and Digital Signature

Sometimes some customers do some activity in the internet through internet banking system and refuse that he has not done this, rather blame the bank officers saying that they could know his Password from the system and do the transactions to transfer money from his account. This is for sure that the bank officer has no access to the customer's Password as all the Password are logically recorded into a system where no bank officer even the administrator has access. Moreover there are electronic records in the system which can easily generate a history of the transactions including name and address of the final beneficiary which will clearly indicates that the bank officer is not a beneficiary. However it becomes very difficult to make this understand to the customers. Digital Signature is a solution to this.

Digital Signature is signing (or encrypting) a message or transaction by sender electronically using his private key which can only be read (or decrypt) by the receiver using the sender's public key. The pair of public and private key is issued by an Issuing Authority (normally a Government Authority, in Bangladesh it is Bangladesh Computer Council) to a user. The user then sends his public key to other users or institutions with whom he wants to exchange electronic information (like email or banking transaction) and keep his private key with him (at his computer or pen drive). Now he will encrypt or sign all the sensitive information using his private key and send to other party. Other party will only be able to open the email or decrypt the information using his public key. This ensures that the transaction is made by the user himself. If the user refuse such transaction, the court can verdict on the issue based on the ICT Act 2006.

Bank can develop a system which will only receive transaction request from the customer which will be encrypted using a private key. All customer desires to do fund transfer transactions using e-commerce may be asked to buy public and private key from the Issuing Authority and submit his public key to the bank.

d) Two-factor authentication

Password can be hacked by a hacker and used for making unauthorized transactions in the internet banking systems. To secure such transactions, banks can introduce 2-factor authentication which means that a customer must authenticate a transaction using two factors – one is Password and another may be a Token which is called Cryptographic or USB or Hardware TOKEN.

Figure: USB Token

A token is a small hardware issued by bank to a customer. The algorithm of the token device and that in the authentication server which records all the token information are same, as such both the server and the token generate same number after every specified time period (say one minute). After submitting the ID and Password, the user gets access to the internet banking system and does many activities except fund transfer and LC transmission. While making a 3rd party fund transfer or transmitting LC, the customer is asked to enter his token number displayed on his token at that particular time. He collects the number from his token and inputs into the system. The internet banking system passes this token number and the token ID into the authentication server which checks for the correctness of the number. If the number is correct the transaction is passed, otherwise rejected.

As the token is a physical device belongs to the user and generates random number, the hacker can capture it but will become invalid in the following minute. Thus the two-factor authentication provides more security for the customers and also protect bank from refusing a transaction by a customer as the token belongs to the customer himself.

7. sms and Alert Banking

7.1. sms Banking

sms Banking is a way of performing some banking activities sending sms from a customer's registered mobile device. It is a push and pull service. The customer must have a deposit account and his mobile number must be linked to the account. On request of the customer, a Bank Officer links the customer's account with a given cell number. The customer is given a PIN which he will use during all the transactions. Each of the messages has some pre-defined syntax. Customer must send the sms as per the syntax. For example if the syntax for a balance enquiry is 'bal <PIN>' and the PIN is 1234, the customer must write the sms like: bal 1234 and send to the bank's short code. If the short code is 3225, the sms should be send to 3225. This short code should be registered with the mobile operator so that the mobile operator will divert all such messages to the bank server using a secured connectivity.
Syntax and example of some of the sms functions are given below:

- Balance Enquiry
  - Syntax: BAL <PIN>
  - Example: BAL 1234
- Statement Enquiry
  - Syntax: STM <PIN>
  - Example: STM 1234
- Payment of Post-Paid Mobile Bills
  - Syntax: PAY <PIN> <Amount> <Mobile #>
  - Example: PAY 1234 200 01911223344
  - Note: If the mobile # is not include, the bill will be paid for the mobile from which the sms is send
- Refill of Pre-Paid Mobile

- Syntax: RFL <PIN> <Amount> <Mobile #>
- Example: RFL 1234 30 01911223344
- Note: If the mobile # is not include, the refill will be done at the mobile from which the sms is send

- PIN Change
  - Syntax: PIN <Old PIN> <New PIN>
  - Example: PIN 1234 4321
- Payment of Utility Bills
  - Syntax: UTL <PIN> <Amount> <Company Code> <account# / customer# / Telephone# / Meter#>
  - Example: UTL 1234 423 101 1.1123456
  - Note: Unique Company code is published by the bank for each of the utility companies
- Payment of Shopping Bills
  - Syntax: POS <PIN> <Amount> <Merchant Code>
  - Example: POS 1234 715 301
  - Note: Unique Merchant code is published by the bank for each of the Merchants

7.2. Alert Banking

Alert is a push service, hence customer does not require to initiate anything for alert. However he will need to register his mobile number with the bank for Alert Services and bank may charge a fee for this service.

The Alert Banking System initiates the alert sms and send to the customers mobile. The system will first send the sms to the Banks short code. The respective Mobile Operator's system will receive the sms and send to the customers mobile.

The system generates three types of alerts and send to the customer's mobile – Debit alert, Credit alert and Periodic alert. The three types of alerts are defined below:

7.2.1. Debit Alert

An auto generated alert sms to the customers mobile when his account is debited for an amount greater than the specified amount. The customer will specify the amount during registration.

7.2.2. Credit Alert

An auto generated alert sms to the customers mobile when his account is credited for an amount greater than the specified amount. The customer will specify the amount during registration.

7.2.3. Periodical Alert

Month-end alert informing month-end balance or for sending any information to the customer's mobile. Such alert sms are initiated by the bank officials.

7.3. How sms Banking works?

Bank installs a software for sms/alert banking at its data center and makes an interface of the sms/alert banking system with the core banking system. Bank also needs to establish a physical connectivity with the mobile operators and makes necessary arrangement for sending and receiving text messages. The mobile operator will allocate a short code to the bank such as 3225.

Now customer types sms as per syntax defined by the bank (say bal 1234) and sends to the short code. The sms will go to the mobile operator's sms server. Mobile operator will add the mobile number from which the sms has been generated with the text (01911223344 bal 1234) and send the entire text to the bank's sms/alert software through the connectivity.

Bank's sms/alert software will do the following:

a) Check if the password (1234) is correct or not.

b) If password is not correct, a message "Incorrect password" will be forwarded to the customer's mobile. If the password is correct, the system will find out the account number which has been linked during registration with this mobile number.

c) From the keyword 'bal' the bank's sms/alert system will understand that the customer wants to know his account balance.

d) The sms/alert banking system will send a request to the core banking system along with the account number of the customer to send back the current balance amount.

e) The Core banking system will find out the current balance and send to the sms/alert banking system.

f) The sms/alert banking system will create a sms using the balance amount, such as "Date: 20/10/2010; Time: 22:23; Ac No: 99999999; BAL: 99999.99 BDT" and will send back to the mobile number using the short code 3225 through the mobile operator.

7.4. Important notes for the customers:

- Please memorize the sms PIN and destroy this.
- Do not disclose the sms PIN to anybody.

- It is recommend that customer changes his PIN frequently.

- As the SMS sent by the customer contains his PIN, it is strongly recommend that the customer deletes the SMS from his “Sent Items” or “Outbox” immediately.

- Banks will not be responsible for any fraudulent activity on the customer’s account due to misuse of his PIN and mobile jointly.

7.5. Security in sms and Alert Banking

sms Banking commands and information are passed from the customer’s mobile device to the bank’s server using ‘Short Messaging System’ which is a simple text. There is no encryption between the mobile and the server. It is also not session oriented. Thus sms banking is not secured.
On the other hand, sms is ‘Store and Forward Data’ service. Thus the entire text of the message including PIN is stored in the mobile set. If not deleted, this can be exposed to other peoples.

Therefore it is desirable that no fund transfer transaction be allowed using sms banking.

8. E-commerce & Internet Payment Gateway

8.1. E-commerce

Buying and selling of goods and services over internet is called e-commerce. The e-merchants do not require to establish shops at the prominent locations of a city. They will have only warehouses in the locations from where they can deliver the goods to the customer’s addresses easily. The customers will place order on-line and pay the bills on-line. The merchant will deliver the goods within a time period declared in the website for the respective items. The requirements for a good e-commerce website are given below:

- The site should display clear pictures of all the items to be sold
- The pictures should be associated with detailed specifications, size, capacity etc.
- Price of each items
- Warranty, if applicable
- Delivery period (may vary location-wise)
- Quantity available at this moment
- Facility for registration of the customers
- The site should be highly secured.

The Internet has created a new economic ecosystem, the e-commerce marketplace, and it has become the virtual main street of the world. Providing a quick and convenient way of exchanging goods and services both regionally and globally, e-commerce has boomed. Today, e-commerce has grown into a huge industry with US online retail generating $175B in revenues

in 2007, with consumer-driven (B2C) online transactions impacting industries from travel services to consumer electronics, from books and media distribution to sports & fitness.

It is important to note that most e-commerce players are at a competitive advantage to retailers. They have lower operating expenses and better inventory management due to operating in a virtual commerce environment. For example, amazon.com has revenue per employee of nearly $850k while its retail counterpart, Best Buy, generates revenue per employee of only $270k.

8.2. Internet Payment Gateway

An e-commerce has life cycle as under:

1. Merchants (sellers) will provide the information in detail of their companies, products and delivery commitments so that the customer can be aware of their products. This can be done through web site.
2. Customer chooses the products and order through the web pages.
3. Payment is made through credit/Debit card through Bank's Payment Gateway.
4. Products is delivered to the customer either through home service or by postal / courier service. The seller should ensure the delivery in time and the quality of the products.
5. Delivery of services during warranty period (if applicable).

Bank comes into picture at stage-3 above. For transferring payment amount from the customer's card account (with bank-A) to the merchant's bank account (with Bank-B or A), bank is involved. For effecting such transfer of fund, Bank installs a special software at it's data center. This software has a link with the merchant's website, Bank's Core Banking System, Credit Card System and the card associations (like Visa and MasterCard).

Therefore an internet payment gateway may be defined as a software installed by a bank at its data center for processing the payments to be made by the cardholders to the e-merchants.

8.3. How Internet Payment Gateway works?

After selection of items to be purchased from a website, the customer clicks at the "Check out" or "Pay" button on the merchant's website. This button contains a computer code called API supplied by the bank which when clicked call a bank's page. In this page, the customer needs to provide his card information such as card number, PIN/CVV/CVC, date of expiry etc. The PIN stands for Personal Identification Number, CVV stands for Card Verification Value & used by Visa and CVC stands for Card Verification Code & used by MasterCard. The price will be shown automatically on the page. This information will be passed on to the Internet Payment gateway software of the bank in a secured way.

The Internet Payment Gateway checks the information for correctness. If the information supplied is found correct, the system debits the buyers bank account or debits card account, and credit the merchant's account. Then the system informs both the parties about the action.

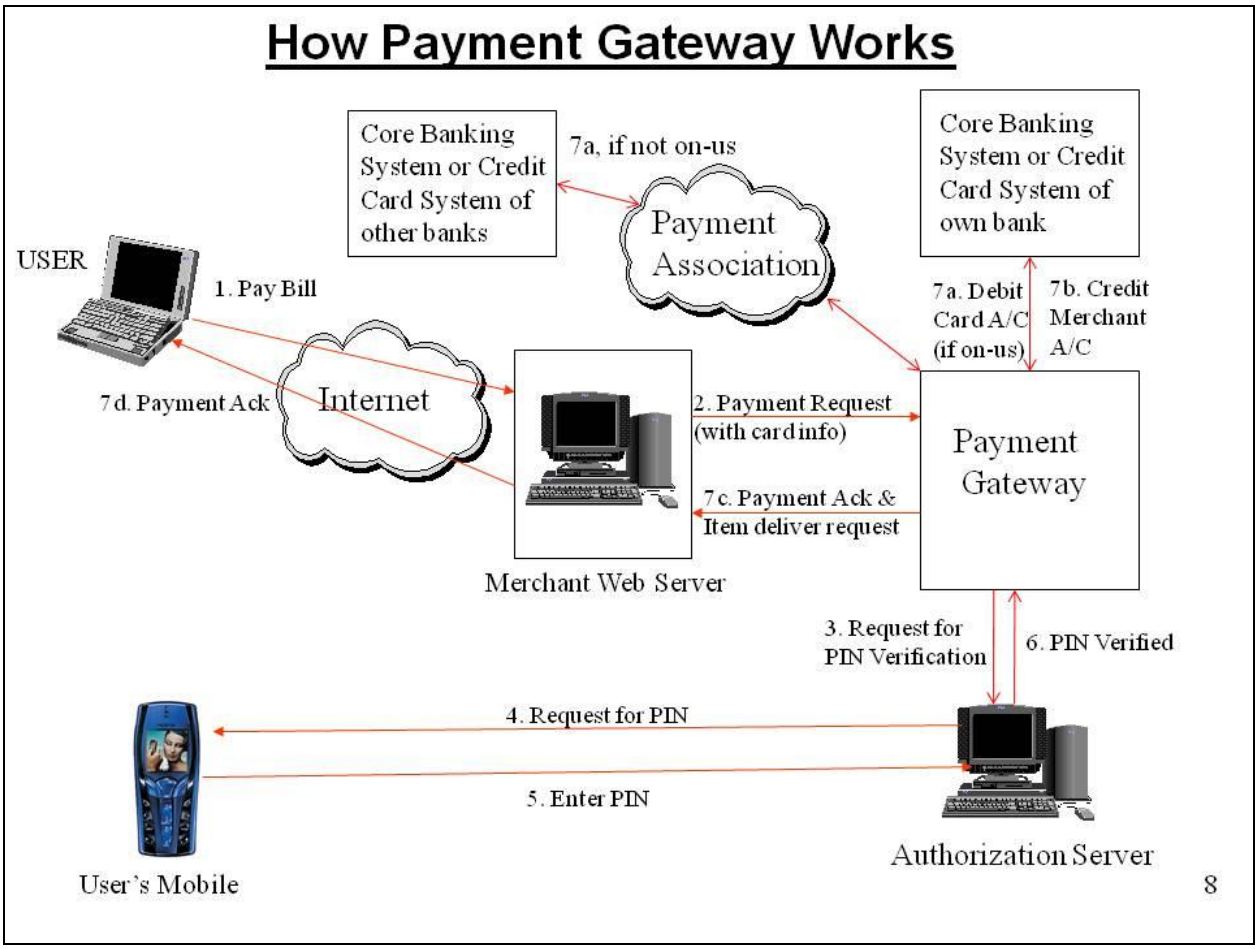
If the card does not belong to the same bank, the payment gateway send the information to the payment association (network of MasterCard, Visa, Amex, JBC, Dinar, Discover etc) where the card belongs to. The payment association then sends the card information to the Issuing Bank. Issuing Bank is a bank which issues the card to the customer.

Now the issuing bank verifies the card information and if found correct, debit the buyer's bank account or card account, and thus authorize the transaction. The authorization message goes to the acquiring bank which then credits the merchant's account and informs both the parties about the action.

The way by which the acquiring bank gets money from the issuing bank, if these are different, is called settlement. The settlement is made daily by the payment associations by debiting the nostro account of issuing bank and crediting the nostro account of the acquiring bank.

Depending on the information obtained from the acquiring bank regarding the action taken, the merchant delivers the goods and services to the buyers address.

The security of the above transaction flow depends on the card information and/or PIN. To make the transaction more secured, some bank introduces 2-factor authentication using a 2^{nd} PIN to be inserted by the customer using his Mobile Device (which is already registered in the system) or inserting into the payment gateway page a variable secure code displayed on a USB Token delivered to the customer by the bank. The 2-factor authentication using an USB Token is described at 5(d) below.



The 2-factor authentication using mobile device is shown in the figure above. Before debiting the customer's account and credit the merchant's account, the Payment Gateway will send a request to an Authorization Server for verifying the customer's authenticity. The Authorization Server, through an IVR, initiates a voice call to the customer's mobile (registered earlier) and requests for PIN. The customer listens to the amount to be deducted from his account and the name of the merchant, and if found correct, type his PIN at the keypad of the mobile device and press send button. The authentication server verify the PIN and if found correct, send the debit and credit request to own host (if on-us transaction) or to the payment association's network (if off-us transaction).

8.4. PayPal as payment gateway:

PayPal has grown in recent years to be one of the most popular methods of online payment. Thousands of businesses accept PayPal payments. If a customer purchases goods and services from such a merchant website linked to PayPal, he can pay using card of any payment association. If the customer is registered earlier, he does not require to give out card or bank account related information to the merchant website, but he will insert only the PayPal account number. Thus the customer's card or bank information will not be exposed to many unknown places.

Because it is not mandatory that the customers be members of PayPal in order to complete transactions, it is possible for the merchant to serve just about anyone. The versatility is one of the reasons that PayPal is so popular as a payment provider. Transactions are secure, and it is generally easy to set-up and integrate PayPal payment options.

One of the main complaints that PayPal users have has to do with the way disputes are settled. There is generally some dissatisfaction with this. Also, with some of the PayPal payment solutions, it is difficult to issue a refund.

8.5. Fraud & remedy during e-commerce transactions

All the transactions of e-commerce are dependent on internet. Internet is a public site. The transfer of card information using interest is not secure. Thus Bank must take adequate measures to secure flow of transaction from customer's computer to Bank server. These measures are described below in brief.

a) Capture of card information during transmission to the bank server

While the card information is travelling through internet from customer's computer to the Bank's server, a Fraudster can easily capture it and use the information to buy valuable goods in the internet or may create a fake card using the captured information, and withdraw money from an ATM. As such while capturing card information from the customer, the bank' system must encrypt them instantly and bring into the server and decrypt them before further processing. If a Fraudster capture encrypted information on the way, it is not possible for him to decrypt and find the real information. As such the information on the way is safe.

b) Phishing

Phishing is collection of user information by presenting a fake web-site address to the internet user. For example, let us consider that the website address of Agora (a merchant) is www.agorabd.com. Hacker will develop a fake website exactly similar to the website of Agora, but with a different address such as www.agora-bd.com and place in the internet. Now if a buyer searches for "Agora" in the Google, address of this fake website will be shown in the search result. Now if the buyer clicks on this link, he will go to the fake website. If he does not look at the website address carefully or address is not known to him, he will select goods and enter card information & PIN into the fake bank web-page. The hacker will record all such attempts made by different users and collect card information.

The false website address may also be send to various users through email where many lucrative offers in the name of Agora may also be communicated. The users, who are not aware of phishing attracts, may login into the false website using the link provided with the email, select goods from lucrative offers, and provide his card information including PIN. All such information will be captures into the hacker's database.

The hacker can now use the collected card information to buy valuable goods in the internet or may create fake cards using the captured information, or withdraw money from an ATM.

It is not possible for customers to know the exact website address of all the merchants. It is also not possible to know the address of the bank to which the merchant is linked as the merchant can be linked to any bank of the world whereas the customer may be using card of a different bank.

It is therefore devised that the website of a bank which collects card information may be certified by a certifying authority such as VeriSign. The page of the bank which collects card information will display seal of the certifying authority. If a customer clicks on the seal, the website of the certifying authority will appears. All the customers must know the web address of the established certifying authority and thus should be able to verify its correctness. If the website address of the certifying authority is correct, the website page of the bank is also correct. As such the customer can insert the card information safely into this webpage.

c) Repudiation and Digital Signature

Sometimes some customers do some activity in the internet through e-commerce or internet banking system and refuse that he has not done this, rather blame the bank officers saying that they could know his PIN from the system and do the transactions to transfer money from his account. This is for sure that the bank officer has no access to the customer's PIN as all the PIN are logically recorded into a system where no bank officer even the administrator has access. Moreover there are electronic records in the system which can easily generate a history of the transactions including name and address of the final beneficiary which will clearly indicates that the bank officer is not a beneficiary. However it becomes very difficult to make this understand to the customers. Digital Signature is a solution to this.

Digital Signature is signing (or encrypting) a message or transaction by sender electronically using his private key which can only be read (or decrypt) by the receiver using the sender's public key. The pair of public and private key is issued by an Issuing Authority (normally a Government Authority, in Bangladesh it is Bangladesh Computer Council) to a user. The user then sends his public key to other users or institutions with whom he wants to exchange electronic information (like email or banking transaction) and keep his private key with him (at his computer or pen drive). Now he will encrypt or sign all the sensitive information using his private key and send to other party. Other party will only be able to open the email or decrypt the information using his public key. This ensures that the transaction is made by the user himself. If the user refuse such transaction, the court can verdict on the issue based on the ICT Act 2006.

Bank can develop a system which will only receive transaction request from the customer which will be encrypted using a private key. All customer desires to do transactions using e-commerce may be asked to buy public and private key from the Issuing Authority and submit

his public key to the bank. This can be made mandatory for transactions above a predefined amount say Tk.50,000.00.

d) Two-factor authentication

Card PIN can be hacked by a hacker and used for making unauthorized transactions in e-commerce and internet banking systems. To secure such transaction over the, banks can introduce 2-factor authentication which means that a customer must authenticate a transaction using two factors – one is PIN and another may be a Token which is called Cryptographic or USB or Hardware TOKEN.

Figure: An USB Token

A token is a small hardware issued by bank to a customer. The algorithm of the token device and that in the authentication server which records all the token information are same, as such both the server and the token generate same number after every specified time period (say one minute). After submitting the PIN, the user is asked to enter his token number displayed on his token at that particular time. He collects the number from his token and inputs into the system. The e-commerce system or the internet banking system passes this token number and the token ID into the authentication server which checks for the correctness of the number. If the number is correct the transaction is passed, otherwise rejected.

As the token is a physical device belongs to the user and generates random number, the hacker can capture it but will become invalid in the following minute. Thus the two-factor authentication provides more security for the customers and also protect bank from refusing a transaction by a customer as the token belongs to the customer himself.

9. M-Commerce and Mobile Financial Services (MFS)

9.1. What is m-Commerce?

Mobile Commerce, also known as M-Commerce or mCommerce, is the ability to conduct commerce using a mobile device, such as a mobile phone, a Personal digital assistant (PDA), a smartphone, or other emerging mobile equipment such as dashtop mobile devices.

Throughout the 1990s the introduction of the internet and ecommerce reshaped the way that businesses do business and the way that consumers interact with businesses. Businesses took the opportunity to automate many processes that before would have been handled manually, from ordering to customer service.

Mobile commerce, often referred to as m-commerce, builds on the advances made by e-commerce (such as automated, electronic processes) but makes interaction available to a wider audience in a more personalized way.

Many more people have access to a mobile phone than to a computers and this means that m-commerce has the opportunity to connect not just big businesses but also small business and consumers on a massive scale. In this sense, mobile phones have the potential to bridge the digital divide and allow organizations and individuals to reach out to one another more easily than ever before.

9.2. History of m-commerce:

Mobile commerce was born in 1997 when the first two mobile-phone enabled Coca Cola vending machines were installed in the Helsinki area in Finland. The machines accepted payment via SMS text messages. The first mobile phone-based banking service was launched in 1997 by Merita Bank of Finland, also using SMS.

In 1998, the first sales of digital content as downloads to mobile phones were made possible when the first commercial downloadable ringtones were launched in Finland by Radiolinja (now part of Elisa Oyj).

Two major national commercial platforms for mobile commerce were launched in 1999: Smart Money (http://smart.com.ph/money/) in the Philippines, and NTT DoCoMo's i-Mode Internet service in Japan. i-Mode offered a revolutionary revenue-sharing plan where NTT DoCoMo kept 9 percent of the fee users paid for content, and returned 91 percent to the content owner.

Mobile-commerce-related services spread rapidly in early 2000. Norway launched mobile parking payments. Austria offered train ticketing via mobile device. Japan offered mobile purchases of airline tickets.

The first conference dedicated to mobile commerce was held in London in July 2001.

The first book to cover mobile commerce was Tomi Ahonen's *M-profits* published in 2002.

The first university short course to discuss mobile commerce was held at the University of Oxford in 2003, with Tomi Ahonen and Steve Jones lecturing. As of 2008, UCL Computer Science and Peter Bentley ran dedicated courses in mobile commerce.

PDAs and cellular phones have become so popular that many businesses are beginning to use mobile commerce as a more efficient way to communicate with their customers.

In order to exploit the potential mobile commerce market, mobile phone manufacturers such as Nokia, Ericsson, Motorola, and Qualcomm are working with carriers such as AT&T Wireless and Sprint to develop WAP-enabled smartphones. Smartphones offer fax, e-mail, and phone capabilities.

Since the launch of the iPhone, mobile commerce has moved away from SMS systems and into actual applications. SMS has significant security vulnerabilities and congestion problems, even though it is widely available and accessible. In addition, improvements in the capabilities of modern mobile devices make it prudent to place more of the resource burden on the mobile device.

9.3. Mobile Financial Services (MFS)

9.3.1. What is Mobile Financial Services (MFS)?

MFS is a banking system mainly for the unbanked population using which a registered mobile holder can deposit & withdraw money from an agent, transfer money from his mobile account to another mobile account, receive remittance from abroad, pay shopping bills & utility bills, receive salary & various government allowances, and top up airtime for his mobile etc.

m-Commerce is a part of Mobile Banking activities. Payment of shopping and utility bills, and airtime recharge refers to the m-commerce activities.

9.3.2. MFS activities:

MFS covers almost all the important retail banking activities such as account opening, cash and transfer. Other two transactions types covered by General (retail) Banking activities of a bank such as clearing and issuance of PO/DD is not possible under the mobile banking scenario. The MFS activities are summarized below:

- Customer registration: Registration of Agents and Merchants by the bank officers and registration of consumers by the Agents. Customer means Consumers, Agent and Merchants.

- Cash : Cash-in/Cash-out through Cash Point (Agent), Bank Branch and ATM

- P2P (Person to Person): Fund Transfer from one customer's mobile account to the mobile account of another customer (domestic remittance). Fund transfer between bank account and mobile account of the same customer is also possible.

- P2B (Person to Business): Utility Bill payment, Educational fee payment, Mobile TopUp, Merchant payment, purchase of Bus/Railway/Airline ticket and Cinema Ticket

- B2P (Business to Person): Salary disbursement by corporate bodies / Industries / Office etc. and sending foreign remittance to the mobile accounts by the foreign exchange houses.

- P2G (Person to Government): Payment of income tax, city corporation tax etc.

- G2P (Government to Person): Disbursement of salary of the primary teachers, elderly allowance and freedom fighters' allowances etc.

9.3.2.1. Agent and Merchant registration:

There are three types of MFS account with three different features. If an account is registered as agent, he will get a menu with three items: Customer registration, Cash-in and Cash-out. If an account is registered as Merchant, he will get only one menu item: Merchant Payment. If an account is registered as Customer he will get menu with several items like: Fund Transfer, Payment of Utility Bills, Payment of Educational fees & charges, Airtime Topup, Purchase a ticket (Bus / Train / Airline / Cinema etc). Some common transactions are: Balance Check, Transaction Inquiry and Change PIN.

Only the designated bank officers can register Agent and Merchant. Bank can nominate and register small shops, Mobile Operator's Retailers, NGO offices and Post Offices at different parts of the country as its agent. These agents are also called as "Cash Point" because customer can deposit money to the Bank or withdraw money from the Bank through these agents.

The Agents can register a Consumer.

9.3.2.2. Consumer Registration:

A consumer fills-up a KYC (Know Your Customer) form and registers for m-Commerce services at any selected agent of the Bank.

The consumer hands over the registration (KYC) form at the agent. The agent invoke the mobile banking menu by sending *<Short Code of the Bank># such as *16216# from his mobile device. The agent then selects 'Registration' from the menu and type the mobile number of the consumer and press send. The Mobile Banking System receives the consumer's cell number. The system then generates a voice call to the consumer's mobile through IVR and informs that he is going to open a mobile account and if he really wants to continue, he should provide a PIN. The consumer (who is in front of agent now) will type his desired PIN at his

Mobile device and continue to listen. In this way the step-1 of the registration process ends. A sms will be sent to the customer informing his account number. The mobile account number is the combination of customer's mobile number and one check digit. If the mobile number is 01233445566 and the check digit is calculated to 8, the mobile account number will be 012334455668.

A mobile number is public and may be known to many people. A check digit prevents sending unwanted money by an unknown person. The customer will share the check digit with only the persons with whom he wants to transact. On the other hand the check digit prevents typing mistake and thus depositing or transferring money to a wrong account.

After completion of step-1 of the registration, the consumer can deposit money to his mobile account, but can't withdraw money from it unless the account is fully authorized. The agents now send the registration forms to the nearby mobile banking office of the bank.

Step-2 of the registration is the data entry by the bank officials or 3rd party agents. Step-3 is checking the consumer's existence and his personal information mentioned in the registration (KYC) form including photograph and signature by a bank officer or 3rd party agent, and authorizing the mobile account in the system. This makes the mobile account fully authorized. The consumer gets a confirmation sms instantly.

9.3.2.3. Cash-in:

Cash-in is the process of depositing money in the mobile account of the consumer. Anybody can deposit cash in a mobile account if he knows the beneficiary's full account number. The agent will issue a deposit slip to the depositor. The account holder will get an instant sms regarding the deposit made into this mobile account.

The consumer hands over money to the agent. The agent invokes the mobile banking menu and selects 'cash-in' from the menu at his mobile device. He types consumer's mobile account number, amount to be deposited and his PIN, and sends to the short code of the bank. The system in the bank's data center will transfer an equivalent amount of money from the mobile account of the agent to the mobile account of the consumer. Therefore the agent can only perform this operation (i.e. receives cash from consumer) if he has sufficient fund in his account. He can re-fill fund into his mobile account from a bank branch or another agent. His mobile account will also be re-filled if he performs cash-out transactions.

9.3.2.4. Cash-out:

Cash-out is the process of withdrawing money from the mobile account by the consumers. Only the account holder can withdraw money from his account. He along with his mobile phone device should physically be present in front of the agent.

The agent invokes the mobile banking menu and selects 'cash-out' from the menu at his mobile device. He types mobile account number and amount to be withdrawn and press the send button. The system in the bank's data center will initiate a voice call to the mobile number of the consumer and inform that he is going to withdraw taka xxxxx from this mobile account and if he wants to continue, he should insert his PIN now. The consumer types his PIN in the keypad of the mobile device. The system checks the PIN and if found correct, it transfers an equivalent amount of money from the consumer's mobile account to the agent's mobile account. Instant sms will be send to both the parties. Then the consumer receives his money from the Agent.

9.3.2.5. Merchant Payment:

Customer buys some items from a merchant and wants to pay from his mobile account. The transaction will be initiated by the merchant from his registered mobile device. He invokes the menu and selects 'Merchant Payment' from the menu options. He types the mobile account number of the consumer and the amount to be paid and press send button. The system in the bank's data center will initiate a voice call to the mobile number of the consumer and inform that he is going to pay taka xxxxx from this mobile account to the merchant yyyy and if he wants to continue, he should insert his PIN code now. The consumer types his PIN code in the keypad of the mobile device and press send button. The system checks the PIN and if found correct, it transfers an equivalent amount of money from the consumer's mobile account to the merchant's mobile account. Instant sms will be send to both the parties. Then the merchant will hands over goods to the consumer.

9.3.2.6. Fund Transfer:

This activity is initiated by the consumer who wants to transfer fund from his mobile account to another mobile account. The consumer invokes the mobile banking menu by sending *<Short Code of the Bank># such as *16216# from his mobile device. The consumer then selects the Fund Transfer menu, types the beneficiary's mobile account number, amount and his PIN code. The system will receive this command and transfer fund from the initiators mobile account to the beneficiary's mobile account. Instant sms will be send to both the parties.

If the consumer selects the 'Fund Transfer to/from Bank account' menu, he will be able to transfer fund between his bank account and the mobile account. Conditions: The consumer must have a bank account and is pre-registered for this service.

9.3.2.7. Other services available to Consumers:

1. A consumer can pay utility bills (electricity, gas, water, telephone etc) and educational fees by transferring money from his mobile account to utility company /educational institution's mobile account.

2. A consumer can buy ticket for bus, train, airplane, cinema and drama by transferring money from his mobile account.

3. A consumer can buy airtime by paying price from his mobile account to the Mobile Operator's account with the bank.

4. Offices, Companies and Industries can disburse salary to their employee's individual mobile account using mobile banking platform.

5. Government authorities can also disburse salary to the primary teachers, disburse elderly allowances, freedom fighter's allowances to the beneficiaries' mobile account using mobile banking platform of a Bank.

6. The Bangladeshi expatriate can send money to mobile banking account of their near and dear ones. The receiver (beneficiary) can withdraw the money from any of the agents, ATMs or branches. This will widen the last mile delivery of remittance.

9.3.3. Who will provide PIN?

The account holder whose account will be debited will provide his PIN to authorize the transaction.

9.3.4. Transaction Limits in MFS:

MFS can't be used for transacting a large amount of money. Bank will set a limit for deposit and withdrawal of money through Agents. Bank will also set the maximum number of transactions that can be performed by a consumer in a day and month. For example an customer may be allowed to withdraw or deposit a maximum of Tk.5,000/- at a time and 5 such transactions in a day but not more than 20 transactions in a month. By setting such limits the bank can reduce risk that may be associated in mobile banking. As the communication using the mobile platform is not 100% secure, the banks do not allow big amount and large number of transactions using mobile channels.

Limits can also be set for agents such as he can't perform 200 cash-in/out transactions in a day and 4000 transactions in a month. Transactions limit will be set for merchants also.

The other limits on consumers may include limitations on amount and number of transactions (in a day and month) for different services like P2P fund transfer, merchant payment, utility bill payment, airtime top up, buying tickets, fund transfer between bank account and mobile account.

9.3.5. MFS is costly:

The customers don't get interest on his deposit in the mobile account. On the other hand the customer needs to pay a fee to the Agents or Bank for transactions in his mobile account. As such the MFS is not cheap for the customers.

Setup and maintaining MFS is costly for Banks. The initial cost is very high due to high cost of necessary software and hardware. Managing a large group of Agents throughout the country is very costly. Bank also needs to engage a large number of employees for verification of KYC physically throughout the country.

9.3.6. Models in MFS: Bank-led and Telco-led:

There are two models of MFS – Bank-led and Telco-led.

In a bank-led model, the bank is responsible for its customers, known as KYC (Know Your Customer), and is the custodian of each customer's money and customer's information. It is established true that the banks are experienced in ensuring proper KYC of the customer. Internal auditors and auditors from the central bank periodically check the complacence of KYC requirement.

For hundreds of years, banks are very much trusted as custodian of the deposits. Central bank has many mechanisms and regulation to ensure that, as and when the customers will ask, a bank will be able to pay the customer's money back. Such mechanisms include maintaining proper liquidity, CAR (Capital Adequacy Ratio), CRR (Cash Reserve Requirements) and SLR (Statutory Liquidity Ratio) by the respective banks. These requirements of the Central Bank help to keep the health of a Bank in good condition and to protect the depositor's interest.

Maintaining secrecy of the customer's information, nature of transactions and balance in the account, is a mandatory requirement of a Bank. This is why no bank can afford to keep its customer database in a shared software or a software system installed and maintained by a third party. All western countries, and our neighbors India and Pakistan, follow some type of bank led model for mobile banking.

On the other hand, in a telco-led model, mobile company is responsible for KYC of the customer, and custodian of the depositor's money and information. However, they should keep an equivalent amount of deposited money with one or more banks (at a negotiated rate of interest). Kenya, Philippines and some other similar countries adopted telco-led model.

In a Bank led model, to protect the customer's deposit and information, the Bank shall ensure the following:

a) The KYC of the customers shall be verified by the bank at its own responsibility before a mobile account is active so that as and when the authority tells the Bank to identify a customer, the bank can do so without fail.

b) The software and hardware system shall be maintained by the Bank to ensure that as and when the authority tells the bank to stop transaction in a particular mobile account, the bank can do so without any dependency on other party, and as and when the authority ask

the Bank to submit transaction history of a particular mobile account, the Bank can submit the same immediately. This is also needed for the safety of the customer data, and confidentiality and security of customer's account.

c) The bank should show total deposit amount of all the mobile accounts in the Balance Sheet of the Bank and thus maintain required CRR (Cash Reserve Ratio) and SLR (Statutory Liquidity Ratio) with Central Bank, maintain required Capital, CAR (Capital Adequacy Ratio) and take such other customer protection measures as per the guideline of the Central Bank.

However, in 2021 the Central Bank of Bangladesh replaced the "Bank-led model" by the "Bank-NBFI-Government-led model". That mean, a Bank or Non-Banking Financial Institutions or Government organization/department having atleast 51% of the share and rest by any entity can form a MFS in Bangladesh.

9.3.7. Connectivity - sms VS USSD:

For connectivity between the mobile banking system at the bank and the mobile device with the agent/merchant/consumer, sms (short messaging system) or USSD (unstructured supplimentary service data) may be used. Sms is not a secured media of comunication, however the USSD is resonably secured. A comparision between sms and USSD channels is given below:

Items	sms	USSD
Data Format	The default data format for SMS messages is in simple plaintext	The default data format is unstructured
Encription	There is no end-to-end encryption between client and bank server	End-to-end encryption presents between client and bank server
Data Storage	SMS is first store data and forward to service	USSD does not store data anywhere
Session	SMS Banking is not session-oriented	Mobile banking is session-oriented such that when a user accesses a USSD service, a session is established, stay connected until customer closes the application

10. Agent Banking

Agent Banking system provides banking services to the doorsteps of the underserved/ disadvantaged segments of the society through engaging outsourced agents. The outsourced agent opens an outlet in the rural area where there exist no bank branches. The agent outlet provides formal banking services on behalf of a bank and bridges the gap between the bank and

the unbanked people of the country. The introduction of agent banking is intended to enable institutions to provide banking services more cost effectively to customers. Transaction process is simplified as well as secured through biometric authentication & done on real time basis and customers can get services at their door steps.

The objective of Agent banking is to provide banking services to people where banking services is yet to reach or where expansion of Bank branches is not financially viable. Agent banking is a cost effective alternative to a bank.

10.1 History of Agent Banking

The idea of agent banking has come from several developing countries of the South America like Brazil, Columbia and Peru. Among the countries, Brazil is recognized as a pioneer of agent banking. Agent Banking first introduced in Bangladesh by the Bangladesh Bank (Central Bank of Bangladesh) in 2013. In this context, Bangladesh Bank later issued a comprehensive Prudential Guidelines for Agent banking operation in Bangladesh in 2017, covering various aspects including the Agent approval process, permissible activities, responsibilities of the banks and agents, AML/CFT requirements, customer protection and business continuity requirements to facilitate safe and effective proliferation of agent banking in the country and has been playing a catalyst in financial inclusion in Bangladesh. Later on other countries like India, Malaysia, Kenya, Pakistan and the Philippines introduced Agent Banking gradually.

10.2 Strategy behind introducing Agent Banking:

Overall strategy behind introducing Agent Banking is to provide a secure alternative delivery channel of banking services to the underprivileged, underserved population who live in remote locations that are beyond the reach of the traditional banking network. The adoption of agent banking mainly geared to improve on market share by attracting and retaining customers, improving financial performance and creating variety of services. Initially agent banking activities were limited with focusing deposit collection and mobilizing but now Agent banking is playing a vital role to strengthen rural economy and facilitating digital Bangladesh through providing banking services including lending among the underserved prospective individuals.

Economic development of the country depends on its rural development. There are 61 scheduled and 5 non-scheduled banks in Bangladesh as of September 2021. The number of banks in Bangladesh is very high compared to the size of the market, but the reach of banking services to the grassroots level is very insignificant. Bangladesh bank has come up with a regulation that, if a private bank wants to open a branch in the urban areas, they need to open

at least one branch in the rural areas. High overhead costs, maintenance, and operational cost of a new branch are some factors that made banks reluctant to open new branches. That's why many of the banks do not have branches even at the district level.

As a result, a large portion of the population from rural areas remained unbanked and out of the scope of financial inclusion. They usually keep their savings with NGOs, Grameen Bank, and other non-bank financial institutions. Banks basically targeted that particular market through agent banking services keeping the interest of various stakeholders. Through Agent banking rural people of the country are getting cash inflow and outflow facilities around the country within shortest possible time. People have engaged with the bank, transaction has increased, huge low cost deposit has been collected, rural people are getting loan facilities and living standard of the people has increased.

Though Agent banking has brought unbanked people under banking umbrella, Banks have a plan to spread the facility to the remote and marginal areas of the country, so that every people get true banking facilities and take part in economic development of the country. Agent banking has the potential to become an alternative attractive financial service channel for rural population.

10.3 Present Scenario of Agent Banking in Bangladesh:

Within just one-and-a-half years of its inception, agent banking has able to attract a huge number of customers, forcing most commercial banks to take up this alternative form of financial service in addition to branch-based banking.

Although the central bank issued an agent banking guideline in 2013, the full-fledged operation of Agent Banking has been started in 2016. The business took off almost immediately opening with 544,536 accounts & deposits of Tk3806.8 million between October and December of that year.

According to June, 2022 quarterly report of Bangladesh Bank, 30 Commercial Banks in Bangladesh have undertaken Agent Banking operation through 19,737 outlets under 14,299 units of agents. And the total number of agent banking account stood at 16,074,378 with deposits of Tk280,853.18 million.

Agent banking has become popular because of its benefits for both banks and clients. Agent banking has able to get such popularity mainly for its simplicity to the clients and cost-effectiveness for the banks. The banks have been able to increase customer volume, improve

financial appearance, lower operating costs, expansion of business, increase deposit collection, improve banks' branding and widen their spreads.

Agent banking has facilitated customers by providing full-fledged banking services at their doorsteps in the remote area, and it has made convenient and easy for channelling remittance.

TilL June 30, 2022, Tk970,481.82 million inward remittances were channelled through 19,737 agent banking outlets across the country.

The agent banking outlets are now not only limited to services like cash deposits, cash withdrawal remittance payment only, the banks have started giving out small loans through the outlets and as of June 30, this year, Tk76,456.33 million loan disbursed through agent banking outlets.

10.4 Agent Banking Model in Bangladesh:

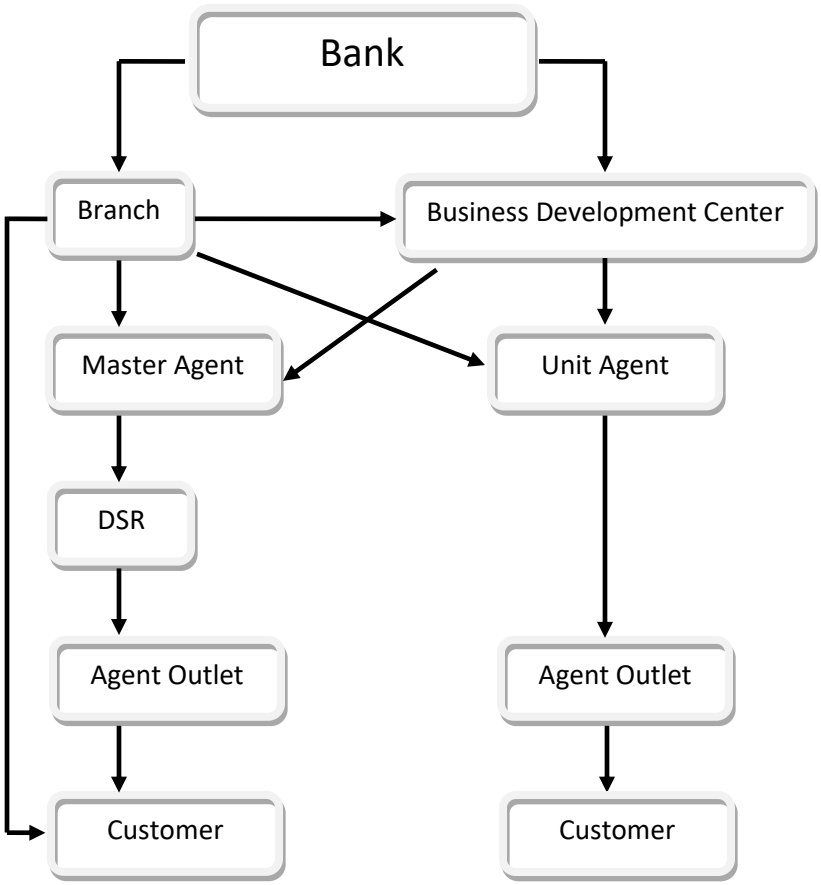
Basically banks are maintaining two types of Agent Banking model for providing services in Bangladesh. One is Distribution Led Model and another is Bank Led Model.

In the Distribution led model, money flows from bank to distributor (Agent) to Outlet to Customer and vice versa. In this model, there are several Business Development Centers throughout the country where the bank's field forces are posted for supervision and Auditing the Agents and Sub-Agents and market development. In this model the Agent works as distributor and its main duty is to rebalance (either supply the short fall of the cash or collect the excess cash) the sub-agents / outlets. Thus outlet does not need to go to the bank branch for rebalancing. However the sub-agents have to share a portion of its income with the Agents.

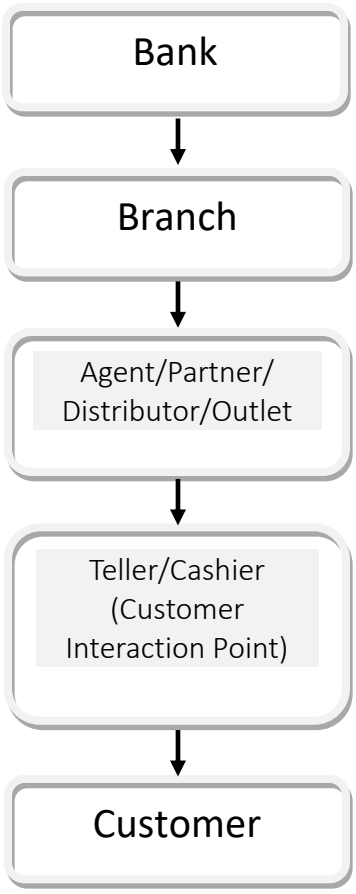
In the unit agent model, the unit agents are outlets which does not carry business under an Agent, but reports directly to the Business Development Office. In this case money flows from bank to Outlet (Unit Agent) to Customer and vice versa.

On the contrary, the Bank led model is almost similar to the Unit agent model, where money flows from bank to Outlet to Customer and vice versa. In the model there is no Business Development Center, but one or two of the Bank's own officials sit in the Outlet and directly monitor and assist the agent outlet. If the branch of a particular bank is far way from the Agent Outlet, it become very difficult to rebalance the cash (either supply the short fall of the cash or collect the excess cash).

Distribution led model



Bank led Model



10.5 Parties involved in Agent Banking:

Agent - Agent refers to the entity which will be appointed by a bank to run the agent banking activities.

Sub-agent – Sub-agent is the entity which will work under the agent and run the agent banking activities in a specific outlet of bank at the customer end point.

10.5.1 Eligible Criteria for Agents/Sub-Agent:

The Banks may engage the following persons/entities as their Agent / Sub-Agent:

i. NGO-MFI's regulated by Micro Credit Regulatory Authority of Bangladesh;
ii. Other registered NGOs;
iii. Cooperative Societies formed and controlled/supervised under Cooperative Society Act, 2001;
iv. Post Offices;
v, Courier and mailing services companies registered under Ministry of post & telecommunications
vi. Companies registered under 'The Companies Act, 1994';
vii, Offices of rural and urban local Government institutions;
viii. Agents of Mobile network operations.
ix. Union Information and Service Centre (UISC);
x. Educated Individuals capable to handle IT based financial services, agents of insurance companies, owners of pharmacies, chain shops and petrol pumps/ gas stations

10.5.2 Criteria for selecting Agent/Sub-Agent:

- Ability to maintain sufficient cash and float balances
- Customer profile suitable to target clients
- Investment capability for new business item.
- Age, education, and experience of proprietor/owner
- Strategic location
- Proximity to Banks/ATMs
- Trust of community
- Business goodwill in local market.
- Social influence.
- Social acceptances.
- Manpower support and Literate staff
- Willingness and motivation of agents for new product etc.
- Adaptability of IT equipment.

10.6 Agent Banking services in Bangladesh:

- Account opening (savings, current, DPS, FDR etc)
- Cash deposit and cash withdrawal;
- Inward foreign remittance disbursement;
- Sourcing, disbursement and collection of repayment of loans;
- Collections of bills/utility bills;

- Collection of insurance premium;
- Payment of retirement and social benefits;
- Payment of salaries;
- Transfer of funds;
- Withdrawal from ATM;
- Balance enquiry;
- Generation and issuance of bank statements;
- Collection of documents in relation to accounts;
- Collect account opening forms, loan application forms, credit and debit card applications;
- Monitoring and recovery of loans and advances sanctioned by the bank; and
- Any other activity as Bangladesh Bank may prescribe from time to time.

10.7 Transaction Process at Agent Outlet:

Agent outlets are permitted to do all types of transactions except foreign exchange transactions and payment through cheque from their Agent outlets. Agent must have to maintain virtual money in his wallet/account for doing all types of transaction. When a customer comes to deposit money to his account, the agent receives the cash and transfer the money to respective account from his wallet/account. Similarly, for withdrawing the money he requires to debit customer account using the fingerprint of the customer and bring the money to his wallet/account to provide the cash. Mentionable that the Agent can use both his wallet or customer account for fund transfer, bill payment and any other transaction by using customer fingerprint or card. When the virtual money of the Agent outlets account got finished he needs to rebalance his account by depositing cash through branches or a distributor.

10.8 Operational Limits (Regulated by BB) for Agent Banking Customer from Agent Outlet

- Banks shall establish limits for the provision of services agreed upon with the agent.
- Banks shall establish limits within which agent shall operate.
- Agent shall open current account(s) with the bank and deposit such amounts as agreed between bank and agent. Initial limits should not be less than BDT2.00 lakh per agent banking outlet. Such limits shall be revised based on demand and transaction profile of the agent.
- Agent shall be responsible for refilling the account(s) to the agreed level of minimum balance as frequently as agreed, however, not less than at least twice a month; once at the half way through the month and the other at the end of the month.
- Banks may also extend credit facility to the agent for meeting unexpected transaction needs, which shall not be more than 100% of the agent's deposit limit with the bank.
- In general, the maximum number and volume of transactions for client at agent

banking outlet should not exceed the limits specified in the following table:

Amount in Lakh BDT

Daily Number of Transactions and Amount Limit						
Nature of Accounts	Cash Deposit		Cash Withdrawal		Transfer/BEFTN/ Inter-bank/Intra-bank	
	Noof transaction	Total Volume	No. of transaction	Total Volume	No. of transaction	Total Volume
Current Account	4	6.00	2	5	4	15.00
Savings Account	2	4.00	2	3	2	5.00
Special Notice Deposit (SND)	4	6.00	2	3	4	10.00

- Transactions beyond the established limits may also be carried but this shall require at least 1 (one) working day prior notice to the bank through the agent.
- In special cases, when a client has need for regular banking transactions exceeding the limits of clause 27.6, banks may set an increased limit for that client with due approval from the Managing Director/Chief Executive Officer of the bank. The increase must be prudent, rational and must accord the merit of the account and client and transaction category based on customer due diligence, client needs and associated risks. Within 30 (thirty) days of such increase of transaction limit, the bank shall inform FID of Bangladesh Bank in writing along with the rationale of such increase with related information of client transactions of at least last 1 (one) month.

10.9 Unique selling proposition of Agent Banking:

- Yearly account maintenance charge Zero.
- Door step service facility by using e-POS
- Inward remittance facility processed by Agent Outlet
- Covered 488 Upazilla out of 493
- Countrywide transaction/service facility including Branch, ATM, FT, Agent Outlet & MBAB office
- Dedicated regional team for customer service and outlet monitoring
- More control over the channel due to business model
- Rebalancing facility through master agent 24/7 specially in remote area
- 365 days open and transaction facility beyond banking hour
- Exclusively operated DBBL agent banking activity

10.10 ROI of Agents/Agent Outlets:

Agents banking opens a profitable business opportunity for the entrepreneurs. Usually, banks provide a fixed commission on the deposit collected by the outlet and disbursement of loan amounts by outlet / sub-agents. In addition, the agent outlet receives a certain amount of transactional charges from every customer's transactions – deposit, withdrawal, fund transfer, utility payment, disbursement of inward foreign remittance etc. They also get commission for opening each of the accounts. However the sub-agents/outlets have to borne the rent, salary of his own officials and utility cost. It has been estimated that a deposit of Taka 5 million in the rural area and 10 million in the urban area is breakeven for a sub-agent.

10.11 Challenges of Agent Banking:

It is somewhat true that, Agent banking poses some challenges which may be depicted as follows:

Technology Related:

- Failure of Customer's Finger print verification from Election Commission's portal
- Birth Certificate & passport verification process fails
- Lack of seamless Internet Connectivity
- Interruption of smooth Electricity supplies
- Periodic evaluation of new technologies
- Fingerprint mismatching for old-aged customers and field workers

Financial Literacy

- Lack of awareness of financial literacy
- Unable to open account due to illiteracy

Competition Aggressiveness

- Multiple Bank's focus on single entity
- Different types of rate for different Banks

Banks & Agents Profitability

- Take longer time to become profitable
- More competition in the same area offered by different banks

Mindset of the rural people

- People in rural areas are still unaware of the banking system
- Some of them are less educated and not comfortable with agent banking

Cash carrying and management risk

- Agents often encounter fraud during carrying cash on their own

11. Call Center

11.1. What is a Call Centre?

A call centre is a customer touch point used for the purpose of receiving and/or transmitting a large volume of sales, requests, complains & quires over phone (by using voice calls only).

11.2. What is a Contact Centre?

A contact centre is a customer touch point used for the purpose of receiving and transmitting a large volume of sales, requests, complains & quires by using multiple communication channels like voice call, fax, email, letter/courier, SMS, web chat etc.

11.3. Difference between Call Centre and Contact Centre

The difference between Call Centre and Contact Centre is the use of technology which is being used to communicate with customers. In Call Centre, only voice call is used as a mode of communication. On the other hand, in Contact Centre multiple communication channels are used as communication channel e.g. voice calls, email, fax, web chat etc.

11.4. Mode of Communication in Contact Centre

- Voice Call: Voice calls are used to communicate to the customer over phone. Different types of voice career e.g. PSTN, GSM, CDMA or VoIP voice communication are used in a contact Centre. Voice calls are used in both inbound and outbound call Centre. Other than voice mode, the rest of the mode of communication in contact Centre is usually referred to as multimedia channels.

- Web Chat: Web chat is something which can be accessed by using internet with the help of a dedicated chat service. By using web chat, customer can access to contact Centre from anywhere in the world. This mode of contact is important for customers who frequently visit/roam around across different geographical location.

- Community Service / Forum / Blog: The most recent tools for contact Centre are community service, forum, blog etc. Unlike other mode of contact, these tools are used to provide solution, to encourage other subscriber's discussion, opinion, experience etc. From contact Centre side, agent guides the discussion, open the topic, provide solution to a post etc. These mode of contact are very useful for technical service contact Canters.

- E-mail is: E-mail is used as one of the multimedia mode of communication. This mode of communication is usually used as a means of serving the off-line customer. Its frequently used to communicate in international contact Centre.

- SMS: Short Messaging Service is frequently used to the contact Centre where poll, public opinion, push pull service etc. are provided. SMS is also effective tool for contact Centre for information dissemination to the customer/target at lower cost.

- Fax: Fax is used as an alternative to the physical paper processing activities e.g. sign on a hard papers to get customer's approval on a particular issues. Two types of Fax can be used in contact Centre like i) Traditional fax, and ii) e-Fax.

- Letter / courier, postal: Contact Centre where physical paper processing is required is suitable for using this mode of contact. Law service, layman customer service etc. Where literacy rate is low, this mode of contact is significantly used in contact Centre.

11.5. Key Components of Contact Centre

11.5.1. Interactive Voice Response (IVR)

IVR handles the calls in an intelligent way where customer can give the input and get the static & dynamic output from the banking systems. Here IVR works as query analyzer. Moreover, IVR gives an option to the customer to talk to the Agent. If customer wants to talk to Agent then IVR handover the call to ACD

11.5.2. Automatic Call Distributor (ACD)

ACD route the calls to the agent based on the defined setting. With an built-in intelligent system it can route the call to an agent under a given criteria. Most common logic is "passing the call to the longer idle agent".

11.5.3. Computer Telephony Integration (CTI)

Once ACD route the call then concerned agent's CTI takeover the call and bring the relevant customer information from different banking systems based on pre-defined queries set by CTI field definitions. Upon population of the customer data it gives call treatment option to the agent.

11.5.4. Call Recording System

All the calls between agent and customer are being recorded with voice and screen recording enabled. 100% call recording is designed for banking call Centre.

11.5.5. Staff (Agent / Supervisors)

Contact Centre's key resource is obviously its human resource. The person who directly serves customers is generally known as "Agent" though they must have a different business designation which is used on cards. A typical contact Centre agent should have nice voice over phone, high level of listening, writing and speaking skills; he must also have positive, proactive and helping attitude while high level of patience is the key success factor to work in contact Centre. One of the critical factors in contact Centre is to identify the right number of agent requirement. Several factors affect calculating the number of agent requirement. These factors included in but not limited to the following;

- Number of Calls Arrival in an hour
- Average Handling Time of a call
- Target Service Level
- Target Call Answer Threshold Time
- Working hour in a shift, number of shifts in a day, working day in a week
- Shrinkage (weekend, holidays in a year, different types of leave quota etc)

Usually, Erlang-C theory is used to calculate number of agent requirement by using above-mentioned information.

Supervisor requirement is determined by the number of agents and by the number of shifts. Usually 08:1 agent: supervisor ration is maintained in a non-technical contact Centre. For technical contact Centre it might be up to 2:1 ration. Supervisors play an important role in contact Centre operations. They are the solution maker and service coordinator of the organizations.

11.5.6. Key Performance Indicator (KPI)

Contact Centre runs by KPI, which indicates how contact Centre agents are spending their time, how they are performing, what level of quality standard are being maintained, how customers are being served, how many customers are smiling after the call is finished etc. All of these questioned can be answered by the KPI. In contact Centre, KPI can be set two different levels like at Agent level and at Supervisor level. Agent level KPIs should include the factors that affect the speed and quality of the service. On the other hand, supervisor KPI includes the factors which can and do affect the contact Centre output e.g. Service Level, ASA, FCR etc. Once the KPI design is perfect, the service goal can be achieved with service provision only.

11.6. How does the Call Centre / Contact Centre function?

Call flow of a Call Centre is narrated below:

1) The customer calls the Call Centre number

2) The call will be routing to BTCL channels from its carriers (PSTN, GSM, CDMA, VoIP)

3) The call then will be carried in to DBBL side trunks using ss7

4) The call then would be landed at IVR, where IVR will treat the customer as per customer's profile and his given input; at this stage customer will get two options:

    i) If customer selects "Self-Service" then he would be served by IVR itself. IVR will retrieve data from different banking systems and will play it to the customer as per customer request. Moreover, IVR will also execute service instructions given by customer himself.

    ii) If customer selects "Assisted Service" then:

        (a) Customer's call will be transferred to ACD where all the agent profiles are kept.

        (b) After getting customer's profile from IVR, ACD will check the agent profile and select the appropriate agent for the call

        (c) Then the ACD will transfer the call to the selected agent's CTI (if there is no free agent then the call will be queued in ACD until a free agent is available)

        (d) CTI will query the banking systems and populate the pre-defined data on agent's CTI screen and give agent option of taking actions (answer the call, reject the call, transfer/forward the calls etc.) on the call

        (e) After closing the call agent will select the reason code of the call and save it to the database

11.7. Types of Call Centre /Contact Centre Service

Call Centre/Contact Centre can play two different types of roles in the organization:

- By providing "Self-Service" through IVR only – here IVR plays relevant information and execute request / instruction as per customer's input.

- By providing "Assisted Service" – here human agents answer the call and do the needful.

In typical call Centre/contact Centre, a mixture of 'self-service' and 'assisted service' is simultaneously to ensure cost effective operation of call Centre.

Key Features of different types of service:

Parameter	Self-Service	Assisted Service
Service Delivery Mode	Interactive Voice Response (IVR)	Call Center Agent
Key Factors to Success	• Ease of Use/ simplicity of IVR flow • Security checking • Availability of Popular Services	• Attitude • Communication • In-depth knowledge • Solution within TAT
Why to Use this Touch Point?	• Cost effective • Ensure participative service delivery • Reduce service delivery risk • Enhancement of service capacity • Always ready service	• To handle customized and complex issues • Complaints handling • Unstructured service delivery (queries etc.) • To serve layman customer

11.8. Call Centre/Contact Centre Activity Type

Based on Call Center/ Contact Center activities we can categorize it in the following group;

Inbound: Only receive calls on queries, request/instruction and complaints

Outbound: Making calls to customers with a view to sales, survey, product promotion, collection etc.

Mixed Mode: Inbound and outbound activities are simultaneously used to ensure best customer experience in terms of service, sales etc.

11.8.1. Common Inbound Activities

- Answer to queries
- Register complaints
- Receive instructions
- Up & Cross selling
- Promote the new products
- Escalation of issues to the concerned authorities
- Manage community service, blog, forum

11.8.2. Common Outbound Activities

- Welcome Calls
- Regular Call Back

- Sale Campaign
- Up & Cross selling
- Special Campaign
- Information Collection & Data Entry
- Customer feedback / satisfaction surveys
- Promotion of new product
- Collection
- Retention

11.9. Quality Assurance at Contact/Call Centre

Quality assurance is the process of monitoring, evaluating and controlling of the service delivery systems & process to ensure that the services are delivered in compliance with the defined service quality standard or not.

- Setting up the standard of service delivery process
- Defining service evaluation mechanism
- Monitoring & evaluating service delivery
- Feedback to agent, supervisor and management regarding service
- Recommend for training
- Investigating service complaints
- Highlighting critical service factors, incidents
- Recommend for process improvement and changes
- Ensure updated product and system knowledge of agents
- Conduct daily clinics

12. Systems for sending fund transfer instruction

12.1. Telex

Banks in Bangladesh are used to send and receive fund transfer or L/C related information to/from a foreign/local bank through Telex. There are a number of reasons for which banks are required to use SWIFT instead of Telex. These are:

(a) The telex messages are not secured. It can be send from any machine located anywhere in the world. Security in telex message is maintained using “test key”. However, a number of frauds have been occurred through transmitting fraudulent messages from telex. In case of SWIFT, only an authorized SWIFT member can transmit a message. Every message has identity indicating from where it has been originated and thus the sender can be made responsible for any occurrence of fraud.

(b) Telex sometimes generates garbage messages for which banks are to request the sender to re-transmit the message. This involves in wastage of time and expenses.

(c) Transmission of message through SWIFT is cheaper than transmission through Telex.

(d) 90% of the banks in the world are using SWIFT. Their banking application software are capable to generate messages in the SWIFT format and send it to the destination without manual intervention. Also these application software can read the message received by the SWIFT from a foreign bank and process it for auto posting of vouchers and generation of various letters, reports and statements. These banks, for sending message through telex, or for further processing of messages received through telex, require extra man-power. Thus they add extra charges for the foreign banks where to be communicated through telex. In near future, no bank will allow such communication, even at an extra charge.

12.2. SWIFT

12.2.1. What is SWIFT?

SWIFT is the abbreviation for "Society for Worldwide Interbank Financial Telecommunication". It is a bank owned co-operative based in Belgium servicing the financial community worldwide. The SWIFT made its debut twenty years back and now it supplies secure messaging and 24-hour global support to 6,495 banks and financial institutes in 178 countries. SWIFT's global network carries an average of 4 million messages in a day. The average daily value of payments messages on the SWIFT network is estimated to be above USD 2 trillion. SWIFT helps its customer reduce costs, improved automation and manage risk. Today, in addition to its 3,000 member banks, SWIFT users include both sub-members and participants such as brokers, investment managers, securities deposit and clearing organisations, and stock exchanges.

12.2.2. SWIFT traffic:

The average daily traffic of the SWIFT is 3.95 million messages with a peak traffic of 4.28 million messages on 29 October, 1998. SWIFT's traffic is distributed over a wide range of financial markets which covers Payments (64.4%), Securities (28.9%), Treasury (10.2%), Trade Finance (5.8%) and others (2.9%). The traffic is high in Europe, Middle-East, Africa region (60.6%) followed by America (20.1%) and Asia-Pacific (15.2%). However, the traffic sent by all customers operating in USA amounts the highest followed by UK and Germany. The routes between UK and USA carry highest number of traffic.

12.2.3. SWIFT membership:

SWIFT defines the three categories of customers as under:

(a) Member:

Any organization which is involved in international financial message transmission, may become a member. For example, DBBL can become a member. In such case all the branches of DBBL in Bangladesh will have the right to use SWIFT services for transmission of Letter of Credit (L/C) and other messages such as fund transfer. Members are the shareholders in SWIFT and thus have voting rights. The member-bank is allotted a 8-digit BIC (Bank Identification Number) such as "DBBL BD DH" for DBBL where BD stands for Bangladesh and DH for Dhaka. The branches will be identified by adding three digits to the BIC. For example, BIC for the Local Office and Agrabad branch of DBBL is "DBBL BD DH 101" and "DBBL BD DH 102" respectively. It may be noted here that the city code for the Agrabad branch, which is located at Chittagong is also "DH".

(b) Sub-members:

Sub-members are either a separate legal entity at least 90% directly or 100% indirectly owned by a member, or foreign branches of a member institution. For example, if DBBL has a branch in USA, that branch can not access SWIFT unless it become a sub-member.

(c) Participants:

The participants are generally one of the following companies:

i) Brokers and Dealers in securities and related financial instruments
ii) Recognized exchanges for securities and related financial instruments
iii) Central depositories and clearing institutions
iv) Money brokers
v) Trust or Fiduciary service companies
vi) Subsidiary providers of custody and nominee services
vii) Registrar and transfer agent organizations
viii) Investment management institutes
ix) Payment system participants
x) Travelers cheque issuers
xi) Trading institutes
xii) Securities electronic trade confirmation (ETC) service provider
xiii) Representative office of a bank or a consortium of banks
xiv) Non-shareholding bank
xv) Non-shareholding financial institutions, and
xvi) Security proxy voting agency

12.2.4. Why to become SWIFT member?

Banks in Bangladesh are used to send and receive fund transfer or L/C related information to/from a foreign bank through Telex. There are a number of reasons for which banks are required to use SWIFT instead of Telex. These are:

(a) The telex messages are not secured. It can be send from any machine located anywhere in the world. Security in telex message is maintained using "test key". However, a number of frauds have been occurred through transmitting fraudulent messages from telex. In case of SWIFT, only an authorized SWIFT member can transmit a message. Every message has identity indicating from where it has been originated and thus the sender can be made responsible for any occurrence of fraud.

(b) Telex sometimes generates garbage messages for which banks are to request the sender to re-transmit the message. This involves in wastage of time and expenses.

(c) Transmission of message through SWIFT is cheaper than transmission through Telex.

(d) 90% of the banks in the world are using SWIFT. Their banking application software are capable to generate messages in the SWIFT format and send it to the destination without manual intervention. Also these application software can read the message received by the SWIFT from a foreign bank and process it for auto posting of vouchers and generation of various letters, reports and statements. These banks, for sending message through telex, or for further processing of messages received through telex, require extra man-power. Thus they add extra charges for the foreign banks where to be communicated through telex. In near future, no bank will allow such communication, even at an extra charge.

12.2.5. Security at SWIFT:

SWIFT maintains various level of security. The operator can only prepare a message. Before posting the message to the SWIFT network, it requires approval from a supervisor. The supervisor approves each of the messages after careful checking and entering his password against each of the messages. There may be more than one level of security for different activities and values. Only the authorized terminal (computer at the member's office) will be able to connect to the SWIFT network, other computers, if try, will be refused. Thus a strict security is maintained.

Moreover, for trouble shooting and maintenance work, two security officers to be nominated – one from the IT department and one from the concern department. They will be provided with part-I and part-II of the security passwords. If any trouble shooting or maintenance work is required, both the officials will have to work together.

12.2.6. How the SWIFT works?

SWIFT is basically a worldwide communication media based on X.25 Public Switch Data Network (PSDN). It is owned and used by the banks and financial institutions. The network has some access points called SAP through which the users enter the SWIFT network. Such two nearby SAP are located in Singapore and Mumbai, India. The member banks in Bangladesh will

make ISD telephone calls to Singapore for submission and receiving of message to/from the Network.

The banks will require to purchase computer, UPS, printer, Leased-line support modem, Eicon card, Windows NT or UNIX software. The quantity will depend on the type of SWIFT alliance software selected by the banks. There are two type of alliance software – alliance entry and alliance access. “Alliance Entry” is a stand-alone software and require one set of hardware and Windows NT. “Alliance Access” is a multi-platform, multi-user software and requires more than one set of hardware depending on the number of messages and branches, and Windows NT or UNIX software. Alliance Access software supports SWIFT operations from terminals in a LAN (Local Area Network), or from computers located in remote branches connected by dial-up/lease-lines and modems. If leased-line is used and WAN be established between the branches, the messages will be routed to the branches automatically. The inward messages will first reach the Head Office and then distributed to the respected branches. The outward messages will be posted by the respective branches to the Head Office server, which in turn will send them to the SAP. Alliance access software can also send/receive messages to/from FAX and telex.

Both the software accept input from banking application software. If the banking software is capable to generate the outward message in SWIFT format, and read and process the SWIFT inward messages, SWIFT operator is not required. This stops posting of various information in duplicate - once in banking application software and again in SWIFT software.

12.2.7. What are the drawbacks?

The SWIFT has some drawbacks. Its one-time cost and annual support charge are high. The one-time membership charge for a bank is around Tk.25 lac and the annual support charge is around Tk.4.5 lac. The banks will also require investment in computers and peripherals. For banks in Bangladesh, the SAP is located in Singapore, thus the banks will require to make an ISD telephone call to the Singapore for collection and transmission of messages. This cost can be reduced if SWIFT install its SAP in Dhaka. Another way is to allow the banks to use X.25 PSDN (Public Switch Data Network) of the BTTB for connection to the SWIFT network. However due to security reason, SWIFT does not agree to provide connectivity with the X.25 network of BTTB. SWIFT has connectivity with the X.25 network of the SITA (which is being using worldwide for the Airline ticketing system). If the banks can arrange connectivity from SITA, SWIFT may allow the banks to connect to the SAP in Singapore using this connection.

12.2.8. User Group in Bangladesh:

First generation banks (cutover in December, 1999): Seven private sector banks in Bangladesh are the first generation members of the SWIFT. The banks are BASIC, Prime bank, AB bank, Islami bank, IFIC, UCBL and NCC bank.

Second generation banks (cutover in June, 2000): Three private sector banks in Bangladesh are the 2nd generation members of the SWIFT. The banks are DBBL, Bangladesh Bank and Dhaka Bank.

Third generation banks (cutover till to date): Rest of the Banks are the third generation members of the SWIFT.

In all countries, where the financial institutes are using SWIFT, there are a few user groups and a national group. In Bangladesh, a first user group was formed with all the first generation participating banks. This user group also represented the national group.

13.3. Bangladesh Automated Clearing House (BACH)

Manual cheque clearing started by Bangladesh Bank immediately after independence, initially at Dhaka, Chittagong, Bogra & Khulna and later expanded to Sylhet, Rajshahi, Barisal & Rangpur. Then further extended to 33 clearing houses in 31 districts run by Sonali Bank on behalf of Bangladesh Bank.

Manual clearing has the disadvantages like:

- Physical movement of Instrument is required
- There is a time delay for several days even within same clearing house
- To clear instruments of outside clearing houses, OBC process takes 1 to 3 weeks' time
- Many manual process & duplication of work
- Weak MIS.

To overcome the above issues, Bangladesh Bank undertook a project for implementation of Bangladesh Automated Clearing House (BACH) in 2006.

BACH has two components:

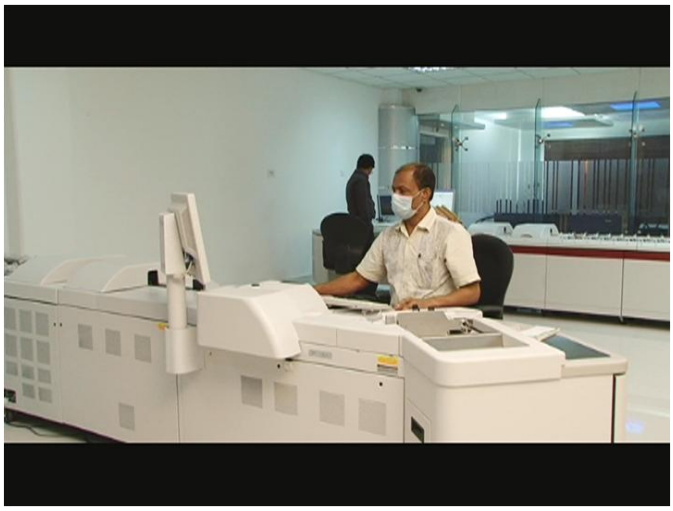
1. BACPS – Bangladesh Automated Cheque Processing System, and
2. BEFTN – Bangladesh Electronic Fund Transfer Network

12.3.1. Bangladesh Automated Cheque Processing System (BACPS)

BACPS is a component of BACH project of Bangladesh Bank. BACPS has completed its rollout at all Bangladesh Bank clearing houses in October, 2011.

Benefits of BACPS:

- ❑ Since Instruments do not travel, it is fast
- ❑ Instruments of any areas are cleared in a day – it is a centralized solution
- ❑ High Value clearing for all areas
- ❑ Higher efficiency, lower cost
- ❑ Higher customer satisfaction
- ❑ Strong MIS



12.3.2. Bangladesh Electronic Fund Transfer Network (BEFTN)

BEFTN went live on February, 2011. BEFTN facilitates the transaction of funds between the banks electronically. It handles transactions like:

- Payroll
- Foreign remittance
- Domestic remittance
- Company dividends
- Retirement benefits
- Corporate payments
- Government allowances

It has countrywide coverage. 100% of the Govt. ministries and departments are disbursing their salaries using BEFTN. A major portion of the foreign remittances are disbursed using BEFTN – when a foreign remittance landed in Bank-A while it's beneficiary maintain an account with Bank-B, then Bank-A will transfer the remittance to Bank-B using BEFTN.

12.4. NPSB

The National Payment Switch Bangladesh (NPSB) is an electronic platform for financial transactions. In terms of card-based and internet-based financial transactions, it links banks in Bangladesh with one another. The card-based financial transactions are made using ATM and POS terminals. Thus a customer of bank-A can use ATM of Bank-B to withdraw money. His account with bank-A will be debited instantly via Bangladesh Bank. Similarly a customer of bank-A can pay his shopping bills from a POS terminal installed by bank-B. The customer can use either a debit or a credit card for card-based financial transaction.

The internet-based financial transaction takes place when the customer uses the Internet banking system of his bank to transfer money to another customer having account with banks-B. In this case, the customer has to use 2FA (2^{nd} factor authentication) to authorize the transaction.

12.5. RTGS

Real Time Gross Settlement (RTGS) systems are funds transfer systems where transfer of money or securities takes place from one bank to another on a "real time" and on "gross" basis. This is the fastest possible money transfer system through the banking channel. Settlement in "real time" means payment transaction is not subjected to any waiting period. The transactions are settled as soon as they are processed. "Gross settlement" means the transaction is settled on one to one basis without bunching or netting with any other transaction. Considering that money transfer takes place in the books of the Central Bank, the payment is taken as final and irrevocable.

12.6. CHIPS

For more than 40 years, CHIPS (Clearing House Interbank Payments System) has set the industry standard for reliability, efficiency and innovation in wire transfer payments. Leading banks worldwide, their correspondents and customers rely on CHIPS for real-time payments that are accurate and final. Today, CHIPS is responsible for over 95% of USD cross-border and nearly half of all domestic wire transactions totaling $1.5 trillion daily.

CHIPS is operated by 'The Clearing House', which also provides ACH, paper cheque exchange and cheque image exchange for financial institutions of all sizes.

12.7. FEDWIRE

Formally known as the Federal Reserve Wire Network, **Fedwire** is a Real Time Gross Settlement Funds Transfer system operated by the Federal Reserve Banks that enables financial institutions to electronically transfer funds between its more than 9,289 participants (as of March 19, 2009).[1] In conjunction with the privately held Clearing House Interbank Payments System (CHIPS), Fedwire is the primary United States network for large-value or time-critical domestic and international payments, and it is designed to be highly resilient and redundant. The average daily value of transfers over the Fedwire Funds Service in 2007 was approximately $2.7 trillion, and the daily average number of payments was about 537,000.

Review Questions

1. Multiple Choice Questions (MCQ)

i) Which one is not an Alternative Delivery Channel?
a) ATM b) Branch c) Agent Banking d) Internet Banking

ii) In which device, cash can be deposited by the customer?
a) ATM b) POS c) CRM d) UPS

iii) Which protocol is used in ATM to communicate with a Switch?
a) TCP/IP b) LAN c) NDC+ d) C++

iv) Which bandwidth is required for ATM communication?
a) 64 kbps b) 1 Gbps c) 16 kbps d) 512 kbps

v) Why a card become a hot card and thus captured by ATM?
a) Insufficient cash in ATM b) Insufficient balance in account
c) Wrong PIN used 3 times d) Wrong amount inserted 3 times

vi) Which of the following is a card fraud?
a) Skimming b) Clustering c) Replication d) Encryption

vii) Which of the following is not a POS transaction?
a) Sale b) Void c) Refund d) Buy

viii) Pre-authorization transaction in POS is usually used in which merchant?
a) Electronic b) e-commerce c) Hotel d) Grocery

ix) The printer used in a POS terminal is called:
a) Dot Matrix b) Laser Jet c) Vacuum d) Thermal

x) The Bank which issue a credit card is called:
a) Issuer b) Acquirer c) Merchant d) Branch

xi) Off-us transactions are also called:
a) Not on-us b) Remote on-us c) Remote off-us d) None of the above

xii) Which one is not a debit card income?
a) Issuance fee b) Renewal fee c) Replacement fee d) Late payment fee

xiii) Internet Banking is also known as:
a) Online banking b) Branch banking c) Smart banking d) Home banking

xiv) Which of the following is not a P2B transaction?

a) Utility Bills Payment b) Mobile TopUp

c) Merchant Payment d) Income Tax Payment

xv) Which of the following is not a category of Swift customer?

a) Member b) Sub-member c) Participants d) Principal member

2. Fill in the gap(s)

i) In case of cash non-dispensed from ATM, the cardholder should report to ……..

ii) Bangladesh Bank is the -------- generation member of use groups of SWIFT in Bangladesh.

iii) BACH has two components: a) -------- and b) ----------

iv) BEFTN went live on --------

v) There are two types of ATMs: Lobby Type and ------ type.

vi) EMV stands for ---------.

vii) ATM safe is available in two standards: UL and -----.

viii) The captured cash of ATM is stored in --------.

ix) POS stands for ---------.

x) A POS terminal can communicate with Data Center using PSTN or ------.

xi) Recording of information on the magnetic strip is called --------.

xii) In the EMVCo, ------, -------, MasterCard and VISA each have 25% share.

xiii) Phishing is collection of ------ by presenting a fake web-site address to the user.

xiv) Buying and selling of goods and services over internet is called --------.

xv) SWIFT stands for ----------.

xvi) BEFTN stands for ----------.

xv) RTGS stands for ----------.

Probable Questions

1. Name 10 channels for alternative delivery of banking services and 7 fund transfer systems.

2. List 5 components of an ATM.

3. What is the function of a cash dispenser in ATM?

4. What services a customer gets from an ATM?

5. How ATM works in case of on-us debit card transaction and on-us credit card transaction?

6. How ATM works in case of not-on-us transaction using an international credit card?

7. Mention the differences between a lobby type and the through-the-wall type ATM.

8. Mention the function of a card reader in ATM.

9. Why a printer is required in ATM?

10. Which technology is used for counting and dispensing money from ATM?

11. Which safe is stronger – UL291 or CEN? Why?

12. Why number of times cash is refilled in CRM is lower than that in ATM?

13. How bank resolve the issue of cash non-dispensed, but account is credited?

14. What is a reject bin and why it is used?

15. What kind of connectivity is use in ATM?

16. What is hot card?

17. List the different expense heads of an ATM booth.

18. How skimming happen and how this can be stopped?

19. ATM + CDM = CRM. Explain.

20. How a POS terminal is used for settlement of merchant bill?

21. How a POS terminal id connected to server in datacenter?

22. Describe following functions of a POS terminals: Sale, Void, Refund, Pre-auth, Cash Advance.

23. Describe how a not-on-us transaction occurs in a POS terminal.

24. Describe the following: PIN Pad, Merchant Commission, Interchange fee.

25. Narrate the different types of frauds found in POS terminal and their remedies.

26.What are the different type of cards? Describe any two of them.

27. Define the following in relation to cards: Issuer, Acquirer, On-Us transaction, Not-on-us transaction, Remote on-us transaction, Charge back.

28. What are the differences between an EMV card and Chip card?

29. What is Liability Shifting?

30. Name five international payment associations. Write a paragraph on any one of them.

31. What are the source of income of a bank from credit card business?

32. What do you mean by card personalization?

33. Define card encoding and card embossing.

34. Write a paragraph on card fraud and its prevention.

35. What are the technological solutions against card counterfeiting?

36. What is EMV? How it is secured?

37. Why banks should move to EMV?

38. What are the standard rules to follow by Internet Banking clients?

39. Mention 3 valid and 3 invalid password for Internet Banking.

40. List a few functions of an Internet Banking.

41. What are the common frauds in Internet Banking and how these can be prevented?

42. How phishing is used in collecting Internet Banking log-in ID and Password?

43. What is a digital signature? Where and why it is used?

44. What is a two-factor-authentication? How this prevent Internet Banking fraud?

45. Mention a few differences between sms and alert banking.

46. Sate the life cycle of an e-commerce transaction?

47. How Internet Payment Gateway works?

48. How an OTP can secure an e-commerce transaction?

49. What are the common frauds in e-commerce transaction and what are the possible remedies?

50. Mention five MFS activities. Describe any two of them.

51. Why transaction limit is imposed in MFS?

52. Why MFS is not cheap for customers?

53. What are the differences among Bank-led, Non-Bank-Led and Bank-NBFI-Govt-Lead MFS models? Currently which model is prevailing in our country?

54. Describe advantages and disadvantages of using sms and USSD as connectivity media for MFS.

55. What is an Agent Banking? What are the objectives of introduction of Agent Banking in Bangladesh?

56. Write a para on the history of Agent Banking.

57. What is the strategy behind introduction of Agent Banking in Bangladesh?

58. Write the resent status of Agent Banking in Bangladesh with respect to Number of Outlets, accounts, banks in Agent banking, and amount of deposit, Credit and inward foreign remittance.

59. Describe Distribution-Led model of Agent Banking.

60. Differentiate between the models: Unit agemt model and bank led model.

61. What are differences among: Agent, Sub-Agent and Unit Agent?

62. What kind of banking services are allowed in Agent Banking?

63. Which banking services are not allowed in Agent Banking?

64. What are the current transaction limits for Savings account holders in Agent Banking?

65. When an Agent Banking become profitable?

66. Mention a few of the challenges of Agent Banking.

67. What is a Call Center?

68. What are the differences between a Call Center and a Contact Center?

69. Name the different modes of communication for a Contact Center?

70. What are the key components of a Contact Center? Narrate them.

71. Present Call Flows of a Call Center.

72. Write key features of self-service and assisted-service of a Call Center?

73. List five common Inbound and five common outbound activities of a Call Center.

74. What do you mean by Quality Assurance at a Call Center?

75. What is the abbreviation of SWIFT?

76. What are the three different categories of membership in SWIFT? Narrate two of them.

77. Why a bank should become a member of SWIFT?

78. Is the SWIFT secured? Why?

79. How SWIFT works?

80. What are the drawbacks of SWIFT?

81. What are the abbreviations of the followings:
    a) BACH, b) BACPS, c) BEFTN, d) NPSB, e) RTGS

82. What are the demerits of manual clearing house? What was the solution to these issues?

83. What are the benefits of BACPS?
84. What transactions can be performed using BEFTN?

Module-D

ICT Security, Cyber Security, ICT Risk Management, Standards, Regulations and Legal Frameworks

1. ICT Security

ICT Security is a security system that is used to secure IT infrastructure, network, data and information of an organization from internal and external treats. This includes physical security, network security, Data Center and DRS security, access control, virus protection, database system security, email security, securing ADCs and bank cards.

Back in 1980, there was no automation of the banking activities in Bangladesh. Large manual ledger was used to record balance of account of customers and transactions such as debit and credit. Interest on account was calculated using calculator result of which was recorded in a large physical ledger. There was no existence of a few words with now-a-day's meaning like Internet, Cyber Security, Hacking, Phishing, Ransomware, Malware, Virus, Antivirus, Firewall, Router.

Gradually, Banks started to introduce software capable of recording account balance, its transactions and calculation of due interest at end of each month. As such job of a banker reduced substantially and bankers were largely happy. These account balance and transactions were recorded in a local hard disk of a computer. There was no need for connectivity with other branch of the same bank.

Later on, other banking activities like General Ledger, Credit functionalities, Foreign Trade functionalities were added in the software which made the bankers more happy and relaxed.

Finally, demand for inter-branch transactions and ATM withdrawal from various clients forced the banks to move to a centralized version of the software which record account balance and transactions of all accounts centrally in a data center. This exposed the database of the bank to the whole country. The branches and the ATMs located all over the country access the central database using wide area network (WAN). The risk of unauthorized access to the database and stealing of customer data (and as such money) become concern for the first time. IT professionals started protecting their database and network placing firewall on the network.

Then demand for accessing account by the clients from home, office or outside the country come up as an important demand. And need for communicating with outside the country for Visa and MasterCard's credit card transaction forced the banks to connect with Internet. The connection of the bank with Internet made whole banking system very vulnerable to security. As a result, hacker from anywhere in the country or in the world can gain access to the banking database if they can find a security lapse in the networking system of the bank.

At this stage, Data Center (DC) became most important part of the IT System of a Bank. To keep the data safe and available in case of any disaster, IT professionals built Disaster Recovery Site (DRS) and Near Data Center (NDC). While DRS is built in a different seismic zone for

data recovery in case of natural disaster, the NDC is built in the same city for quick start of the operation in case of major or minor breakdown in the DC.

Having all the technological innovations in place in the Banks in Bangladesh, the threats may be categories as under:

1.1. Business Continuity Threats

This is one kind of treat occurs from server or equipment failure in the Data Center for which the system remains unavailable to the users and customers. The users in the branches can't provide banking services to the customers. Also the customers can't make transactions in ATM, POS, e-commerce site or internet banking. Customers become dissatisfied and may leave bank if bank can't ensure business continuity. The business discontinuity may be classified as under:

a) Simple Breakdown:

Due to simple breakdown in the Data Center, system may remain unavailable for a few minutes to hours. The causes for such breakdown and its remedies are given in table-1.

Table-1:

Causes	**Remedies**
Server Non-Functioning	• Active-Active Clustering – for database servers • Network Load Balancing (NLB) – for application servers
Network Equipment	Redundant active-active network equipment
UPS	Redundant UPS
Cooling System	Active-Standby

b) Major Shutdown:

Due to major breakdown in the Data Center, system may remain unavailable for several hours or weeks. The causes for such breakdown and its remedies are given in table-2.

Table-2:

Causes	Remedies
Database (DB) Corrupted	✓ Establishment of Near Data Center ✓ To have the functionality of going back to a specific time period in the storage
Storage Corrupted	✓ Establishment of Near Data Center ✓ RMAN base backup in a separate storage in the same DC or Near DC
Datacenter damaged by fire	Establishment of a Near Data Center

c) Data Center Collapsed due to Natural Calamity like Earthquake, Flood and Cyclone:

In case the Data Center is collapsed due to natural calamity like earthquake, flood and cyclone, the system may remain unavailable for a week to months. To keep the business continued in such case, it is highly recommended to build a Disaster Recover Site (DRS) in a different seismic zone and a Near Data Center (NDC) in the same city with the same capacity and connectivity as in the Data Center.

1.2. Internal Threats

a) Unsatisfied or Corrupt Employee:

Unsatisfied employee or corrupt employees in a Bank may steal data or information and handover to the hackers.

b) Database Breaching:

If a Database which stores sensitive banking or credit card data is easily accessible to many administrators of the bank (sharing same password), it may lead to stolen of data or intentional damage of data. In such case, it is difficult to identify the administrator responsible for this.

1.3. Mobile Financial Services (MFS) related Risks

Mobile Financial Services itself has risk of unavailability of service due to threats narrated above. However, it has brought new type of risks to the customers and the country. These are presented in Table-3.

Table-3:

Risks to the customers or country	Remedies
SIM Cloning and withdrawal of money from MFS customer's account	When original SIM is replaced by a new SIM at a MNO retailer, MNO shall send the information to the MFS provider. MFS provider to block the account immediately. Then, MFS provider unblocks the account only after receiving a call from the genuine SIM holder.
Extortion / Blackmailing /Deceiving / Making Fool of MFS customers	By way of extortion etc, the money from MFS customer's account is transfer to another account (KYC of which is false). Later on, although the destination account can be detected, the owner remains unidentified. This can be minimized by:- ✓ NID verification before activation of MFS account ✓ Properly filled-up KYC Also awareness campaign can help to educate customer not to be deceived.
Receiving bribe, collection of money for human trafficking & drug selling, terrorist financing using MFS	MFS account may be used for collection of illegal money. In many cases the owner of such account can't be detected due to wrong account opening information available in the database. This can be reduced by following measures: ✓ NID Verification before activation of MFS account ✓ Arresting OTC (Over The Counter) Transactions ✓ Use of Sanction Screening System & Transaction Monitoring Software
Digital Hundi using MFS and as a result country is deprived of foreign currency	Digital Hundi is sending foreign remittance illegally through MFS. Due to rampant Digital Hundi, a 17% fall in inward foreign remittance was recorded in 2017. To stop digital hundi as well as other irregularities as mentioned above, direct cash-out from Agent may be discontinued. Cash-out may be made through a registered bank account with any bank. This will stop all misuse of MFS and in the same

Risks to the customers or country	Remedies
	time, will increase electronic use of wallet – will make a 'real less cash Bangladesh'.

1.4. ATM / POS / e-COM / Card related Treats

1.4.1. ATM Skimming:

ATM and POS are vulnerable to skimming. Skimmers attach a device on the card slot of an ATM and collect card information. A camera is used to record ATM PIN. Then the fraudster creates a duplicate card (called **card cloning**) using the collected information and withdraws money from ATM using the card and PIN.

Use of Anti-Skimming device in the ATM can prevent copying card data to a Skimming device. Another way to handle this is to issue chip card to the customers. Skimming device can't copy data from chip of a debit or credit card.

1.4.2. POS Skimming:

Some corrupted salesman in super shops also keep skimming device under his table and sweep the customers card in the skimming device before he really use it in the POS terminal on the table. In this way, he collects card information, creates a card using the collected information and uses the created clone card in a POS terminal to buy gold or costly electronic items.

This type of fraud can only be arrested by issuing chip card to the customers. Skimming device placed under the table will not be able to copy data from chip of a debit or credit card.

1.4.3. ATM Jackpotting:

If hackers can gain control of the ATM controller (called Switch), he can send signals to the ATM machine which indicates that ATM has to dispense money. In this way, the ATM start dispensing money without any card and an associate of the hacker collects the cash and go away. This is called ATM Jackpotting.

To protect the ATM controller from such kind of Hackers, it is necessary to prevent unauthorized access to the computer network of the bank.

1.4.4. e-commerce fraud:

In e-commerce site, payment can be made using three pieces of card information: Card number, expiry date and a 3-digit secrete number. All these information are written on a

card. When a card is handed over to a waiter in a restaurant, he can note all these information and make e-commerce transaction later on.

To prevent such unauthorized use of card information in an e-commerce site, the card issuing bank may deliver 2FA (2^{nd} factor authentication) token to the cardholder and the e-commerce acquiring bank must ask for 2FA number in addition to the three piece of information. The 2FA token number is an one-time number and can be generated on a pen-drive like device or by an Apps installed on the customer's smart phone/laptop. It can also be an OTP (one-time password) send from issuing bank to the mobile of the cardholder.

1.5. External Risks / Cyber Threats

1.5.1. Distributed Denial of Service (DDoS):

A DDoS attack is done by unknown attackers to shut down a website, machine or network of a bank, making it inaccessible to its clients. Installation of appropriate network security system can prevent DDoS attack in a bank.

1.5.1. Ransomware:

Ransomware is a type of malicious software that blocks access to the users in to their system or computer unless a ransom is paid. The malicious software is first send to many employees of a Bank as attachment of an email narrating attractive offers. If an unconscious user clicks the email attachment, the malicious software automatically gets installed in the computer. The software then spread over the WAN to all the computers. The software than encrypt all or selected files in the computer. The key to unlock the files is handed over by the Hacker to computer's owner only if demanded ransom is paid. Normally ransom is paid in crypto-currency like Bitcoin.

Awareness program may be run among the employees of a bank to educate them so that they will not click on the unknown attachments of email.

1.5.3. Malware:

Malware is a program that embeds itself in some other executable software (including the operating system itself) on the target system without the user's consent and when it runs causes the malware to spread to other executable.

The malware is first sent to many employees of a Bank as attachment of an email narrating attractive offers. If an unconscious user clicks the email attachment, the malware automatically gets installed in the computer. The malware then start sending all the sensitive information including user ID and password to the hacker.

The other away of infecting a computer is called Phishing. Phishing is presenting a fake website, the look and feel of which is like a real one and the user enter personal information in to the fake site which is captured by the hacker.

Using the information so far received, the hacker gains access to the user's sensitive system and transfer fund from a customer's account to another bank account or withdraw money directly from the hacked account.

Awareness program may be run among the employees of a bank to educate them so that they will not click on the unknown attachments of email and they don't input their user ID and password to a website without proper verification.

1.6. Hacking and Unauthorized Transfer of Money:

The hacker constantly tries to gain access to the banking system for years together. If he can find a loophole in the security system, using that loophole the hacker gets access in to the banking network. Then he transfers fund from a customer's account to another bank account or withdraw money directly from the hacked account.

Bangladeshi Taka is non-convertible. So fund transfer from CBS (Core Banking System) is not attractive to the attackers / hackers. After transferring fund from a client's account to the hacker's account, the hackers need to withdraw Taka from a bank branch or ATM within Bangladesh and then convert taka to USD from an exchange house. And finally take USD physically outside the country. The process is complex & risky, and as such hackers are less interested in hacking any CBS of a Bangladeshi Bank.

However, SWIFT system and Credit Card System maintain customer's balance in USD and are vulnerable. If hackers can gain access to SWIFT or Credit Card System, they can transfer USD directly to another account anywhere in the world and withdraw money of that particular country. They can also withdraw USD from ATM in USA.

The IT Security Department of a bank needs to continuously analyze the pattern of different unsuccessful attacks and makes the Banking network robust and secured applying different policies.

1.7. Stealing Credit Card Data:

Hackers steal credit card data from the database. Using the stolen Credit Card Data, the hackers create fake credit cards and then use them for purchase / withdrawal of money (get taka in Bangladesh or other currency in other countries).

Installation of appropriate network security system by the IT Security Department of a Bank can prevent hackers from stealing credit card data.

1.8. Crypto-Currency Threats

Crypto-currency is an electronic version of cash. Examples of some of the crypto-currencies are - Bitcoin, Ether, Litecoin, Monero, Dash, PonziCoin, Zcash, Carbon, Tether and Petro. The owner of a Crypto-currency remains anonymous in the system (as no KYC is done for the user during onboarding) and as such it is used for payment of various illegal activities such as for buying drugs and other illegal goods, payment of ransom, transfer of money against human trafficking and payment to organized terrorist groups. Some of the backdrop of Crypto-currency are:

- It is not controlled by a Central Bank
- It has no geographical boundary
- The users don't require any KYC
- It has no specific authority, thus no consumer protection and no AML/CFT reporting
- Like real money, the value of a crypto-currency is not backed by any assets

As such the Crypto-currency has failed to become a currency.

The main threat of Crypto-currencies is the Money Laundering and Terrorist Financing (MLTF) risk.

1.9. What to do to minimize the risk?:

To minimize the threats arises from Banking Automation, it is required by the banks to setup an independent IT Security Department (under MD & CEO). Also the Banks need to ensure the followings:

- Setting up Data Center, DRS and Near Data Center at appropriate locations with full range of servers, equipment and networking,
- Conducting employee awareness program,
- Setting up well structured IT infrastructure,
- Obtaining PCI-DSS and ISO27K certification,
- Placing and configuring the following network equipment properly
    - Firewall
    - IPS
    - WAF (web application firewall)
    - Email security gateways
    - Web Security gateways,
- Not to use pirated software,
- Updating drivers regularly,
- Reviewing patches regularly,

- Taking measures to stop zero-day attracts (sandboxing), and
- Regularly investigating with Cyber Security experts

2. Cyber Security

Cyber security is a security system used to protect data and information of an organization from unauthorized external electronic access normally using Internet. Cyber Security is a subset of ICT security. Small businesses are more vulnerable to cyber threats as potential hackers know small businesses lack in resources substantially as large corporations do to invest in security technologies and strategies. Security procedures and policies protecting digital networks change rapidly so businesses need to stay up-to-date with the latest cyber security measures to better defend their cyberspace against cyber threats. Some of the most common cyber attacks include phishing, data breaching, baiting, etc.

These are discussed in the previous section.

3. ICT Risk Management

ICT risk management is referred to as the essential process developed by an organization to protect its ICT systems. As per the requirement of the Central Bank of Bangladesh, as part of ICT risk management process, each of the Banks and NBFIs in Bangladesh need to develop their respective ICT policies, obtain approval of their respective Board of Directors and implement into their ICT systems.

4. Security Standards and Regulations

Many governments around the world are preparing or have adopted **standards** (which the enterprises may follow to improve their IT security) **/ regulations** (which the enterprises must follow to avoid penalties) prescribing how companies should manage and control information security. The aim is simple: compel management and boards of directors to be responsible for information security, and encourage them to display the same "due diligence" they devote to protecting their assets.

Such regulations include Sarbanes-Oxley Act of 2002 (**SOX**), the Gramm-Leach-Bliley Act (**GLBA**) and the Health Insurance Portability and Accountability Act of 1996 (**HIPAA**), USA **Patriot Act**, Canada **PIPEDA** and standards include **BS7799** (or ISO17799), "**Guideline on ICT Security for schedule Banks and Financial Institutions**" framed by the Bangladesh Bank (Central Bank of Bangladesh) and many national standards.

A brief comparison of some of the Security Standards / regulations is given below:

Security	Who should comply?	What do the	What are the	When is it in

Regulations / Standards		security provisions cover?	penalties?	Effect?
Sarbanes-Oxley Act of 2002	All public companies subject to US security laws	Internal controls and financial disclosures	Criminal and civil penalties	Current law
Gramm-Leach-Bliley Act of 1999	Financial institutions	Security of customer records	Criminal and civil penalties	Current law
Health Insurance Portability and Accountability Act (HIPAA)	Health plans, health care clearinghouses, and health care providers	Personal health information in electronic form	Civil fines and criminal penalties	Current law
BS7799 / ISO 17799	Any enterprise interested in improving IT security	Information Security Management System (ISMS) of any enterprise	Not a law, thus no penalty provision	Current Security Standard
Guideline on ICT Security for schedule Banks and Financial Institutions	Banks and financial institutes in Bangladesh	Security of IT assets and customer data	Not a law, thus no penalty provision	Current Security Standard
PCI-DSS	Any organization dealing with debit and credit cards.	Securing flow and storage of card related data and information	Not a law, thus no penalty provision	Current Security Standard
ISO 27000	Any enterprise interested in improving IT system and security	ICT systems of any enterprise	Not a law, thus no penalty provision	Current Security Standard

An organization that complies with any one of these standards / regulations already possesses a concrete and practical information security management system.

For example, HIPAA tackles the same subjects as the ISO 17799 standard while placing the emphasis on the protection of private information. Compliance with ISO 17799 and BS7799-2 can include the definition of policies and procedures for the security of a company's sensitive information, as touched on in SOX.

In this chapter we will discuss on the Security Standards, specifically on the **"**Guideline on ICT Security for schedule Banks and Financial Institutions" published by the Bangladesh Bank and the BS7799 and ISO 27000.

Benefits of complying a Security Standard

Obviously, complying with a Security Standard and obtaining "certification" on a certain standard does not in itself prove that an organization is 100% secure. The truth is, barring a

cessation of all activity, there is no such thing as complete security. Nevertheless, adopting a standard confers certain advantages that any manager should take into consideration, including:

At the organizational level

Commitment: certification serves as a guarantee of the effectiveness of the effort put into rendering the organization secure at all levels, and demonstrates the due diligence of its administrators.

At the legal level

Compliance: certification demonstrates to competent authorities that the organization observes all applicable laws and regulations.

At the operating level

Risk management: leads to a better knowledge of information systems, their weaknesses and how to protect them. Equally, it ensures a more dependable availability of both hardware and data.

At the commercial level

Credibility and confidence: partners, shareholders and customers are reassured when they see the importance afforded by the organization to protecting information. Certification can help set a company apart from its competitors and in the marketplace.

At the financial level

Reduced costs related to security breaches, and possible reduction in insurance premiums.

At the human level

Improves employee awareness of security issues and their responsibilities within the organization.

5. Guideline on ICT Security for Scheduled Banks and Financial Institutions published by the Central Bank of Bangladesh (2015)

The banking industry has changed the way of providing services to their customers and processing of information in recent years. Information and Communication Technology (ICT) has brought this momentous transformation. Electronic banking is becoming more popular and enhancing the adoption of financial inclusion. Security of Information for financial institutions

has therefore gained much importance and it is vital for us to ensure that the risks are properly identified and managed.

Moreover, information and information technology systems are essential assets for the Banks and Non-Bank Financial Institutions (NBFIs) as well as for their customers and stakeholders. Information assets are critical to the services provided by the Banks and NBFIs to their customers. Protection and maintenance of these assets are important to the organizations' sustainability. Banks and NBFIs must take the responsibility of protecting the information from unauthorized access, modification, disclosure and destruction. Approaches of Banks and NBFIs for business leading to services are risk-based, which means ICT risk is also associated with banking system that needs to be managed with thoughts and efforts. I view to this, a Guideline on ICT Security has been developed by the Bangladesh Bank in 2015 to follow by the Banks and NBFIs. The silent features of the Guideline will be discussed in this chapter.

5.1. Categorization of Banks and NBFIs

Depending on the architecture of core business application solution, ICT infrastructure, operational environment and procedures, a Bank or NBFI can be categorized as follows:

Category-1: Centralized ICT Operation for managing core business application solution through Data Center (DC) with backup assets for continuation of critical services including Disaster Recovery Site (DRS) / Secondary Data Center to which all other offices, branches and booths are connected through WAN with 24x7 hours attended operation.

Category-2: Decentralized ICT operation for managing distributed business application solution hosted at DC or operational offices/branches with backup assets for continuation of critical services connected through WAN or having standalone operations.

5.2. ICT Security Management

ICT Security Management must ensure that the ICT functions and operations are efficiently and effectively managed. Banks and NBFIs shall be aware of the capabilities of ICT and be able to appreciate and recognize opportunities and risks of possible abuses. They have to ensure maintenance of appropriate systems documentations, particularly for systems, which support financial transactions and reporting. They have to contribute in ICT security planning to ensure that resources are allocated consistent with business objectives and to ensure that sufficient and qualified technical staffs are employed so that continuance of the ICT operation area is unlikely to be seriously at risk. ICT Security Management deals with Roles and Responsibilities, ICT Security Policy, Documentation, Internal and External Information System Audit, Training and Awareness, Insurance or Risk coverage fund.

5.2.1 Roles and Responsibilities

Well-defined roles and responsibilities of Board and Senior Management are critical while implementing ICT Governance but clearly-defined roles enable effective project control and expectations of organizations. ICT Governance stakeholders include Board of Directors, CEO, ICT Steering Committee, ICT Security Committee, CIO, CTO, CISO, Risk Management Committee, Chief Risk Officer and Business Executives.

i) Roles and responsibilities of Board of Directors

a) Approving ICT strategy and policy documents.

b) Ensuring that the management has placed an effective planning process.

c) Endorsing that the ICT strategy is indeed aligned with business strategy.

d) Ensuring that the ICT organizational structure complements the business model and its direction.

e) Ensuring ICT investments represent a balance of risks and benefits and acceptable budgets.

f) Ensure compliance status of ICT Security Policy.

ii) Roles and responsibilities of ICT Steering Committee

ICT Steering Committee needs to be formed with representatives from ICT, Risk, HR, ICC/Audit, Legal and other related Business units.

a) Monitor management methods to determine and achieve strategic goals

b) Aware about exposure towards ICT risks and controls

c) Provide guidance related to risk, funding, or sourcing

d) Ensure project priorities and assessing feasibility for ICT proposals

e) Ensure that all critical projects have a component for "project risk management"

f) Consult and advise on the selection of technology within standards

g) Ensure that vulnerability assessments of new technology is performed

h) Ensure compliance to regulatory and statutory requirements

i) Provide direction to architecture design and ensure that the ICT architecture reflects the need for legislative and regulatory compliance

iii) Roles and responsibilities of ICT Security Committee

ICT Security Committee needs to be formed with representative from ICT, ICT Security, Risk, ICC and Business units.

a) Ensure development and implementation of ICT security objectives, ICT security related policies and procedures.

b) Provide ongoing management support to the Information security processes.

c) Ensure continued compliance with the business objectives, regulatory and legal requirements related to ICT security.

d) Support to formulate ICT risk management framework/process and to establish acceptable ICT risk thresholds/ICT risk apatite and assurance requirements.

e) Periodic review and provide approval for modification in ICT Security processes.

5.2.2 ICT Policy, Standard and Procedure

i) Each Bank or NBFI must have an 'ICT Security Policy' complied with this ICT Security Guideline and be approved by the board.

ii) The policy requires regular update to deal with evolving changes in the ICT environment both within the Bank or NBFI and overall industry.

iii) Bank or NBFI shall engage ICT security professional employed in separate ICT security department/unit/cell for improved and impartial dealing with security incidents, policy documentation, inherent ICT risks, risk treatments and other relevant activities.

iv) For noncompliance issues, compliance plan shall be submitted to Bangladesh Bank for taking dispensation. Dispensation shall be for a specific period of time.

5.2.3 Documentation

i) Bank or NBFI shall have updated organogram for ICT department/division.

ii) Bank or NBFI shall have ICT support unit/section/personnel (Business/ICT) in the branch organogram.

iii) Each individual within ICT department/division/unit/section shall have approved Job Description (JD) with fallback resource person.

iv) Bank or NBFI shall maintain segregation of duties for ICT tasks.

v) Bank or NBFI shall maintain detailed design document for all ICT critical systems/services (e.g. Data Center design, Network design, Power Layout for Data Center, etc.).

vi) Bank or NBFI shall have prescheduled roster for sensitive ICT tasks (e.g. EOD operation, Network Monitoring, Security Guard for Data Center, ATM Monitoring, etc.).

vii) Bank or NBFI shall maintain updated "*Operating Procedure"* for all ICT functional activities (e.g. Backup Management, Database Management, Network Management, Scheduling Processes, System Start-up, Shut-down, Restart and Recovery).

viii) Bank or NBFI shall have approved relevant requisition/acknowledgement forms for different ICT request/operation/services.

ix) Bank or NBFI shall have User Manual of all applications for internal/external users.

5.2.4 Internal Information System Audit

i) Internal Information System (IS) audit shall be carried out by Internal Audit Department of the Bank or NBFI.

ii) Internal IS audit shall be conducted by personnel with sufficient IS Audit expertise and skills. Engagement of certified IS auditor having adequate audit experience in this area of technology will be appreciated.

iii) Bank or NBFI may use Computer-Assisted-Auditing Tools (CAATs) to perform IS audit planning, monitoring/auditing, control assessment, data extraction/ analysis, fraud detection/prevention and management.

iv) An annual system audit plan shall be developed covering critical/major technology-based services/processes and ICT infrastructure including operational branches.

v) Internal Information System audit shall be done periodically at least once a year. The report must be preserved for regulators as and when required. Bank or NBFI shall also ensure that audit issues are properly tracked and, in particular, completely recorded, adequately followed up and satisfactorily rectified.

vi) The bank/branch or NBFI shall take appropriate measures to address the recommendations made in the last Audit Report (external/internal). This must be documented and kept along with the Audit Report mentioned in 2.4.5.

5.2.5 External Information System Audit

i) Bank or NBFI may engage external auditor(s) for their information systems auditing in-line with their regular financial audit.

ii) The audit report shall be preserved for regulators as and when required.

5.2.6 Standard Certification

Bank or NBFI may obtain industry standard certification related to their Information System Security, Quality of ICT Service Delivery, Business Continuity Management, Payment Card Data Security, etc.

5.2.7 Security Awareness and Training

i) As technology evolves rapidly, Bank or NBFI shall ensure that all relevant personnel are getting proper training, education, updates and awareness of the ICT security activities as relevant with their job function.

ii) Bank or NBFI shall also ensure the minimum level of Business Foundation Training for ICT personnel.

iii) Bank or NBFI shall arrange security awareness training/workshop for all staff.

iv) Bank or NBFI shall ensure adequate training/awareness facilities for IS Audit team considering any new banking services and technological changes.

5.2.8 Insurance or Risk Coverage Fund

i) Adequate insurance coverage or risk coverage fund shall be maintained so that costs of loss and/or damage of the ICT assets can be mitigated.

ii) The risk coverage fund shall be maintained properly in the accounting system of Bank or NBFI, if applicable.

iii) There shall have a clear policy to use risk coverage fund at necessity if it is maintained.

5.3. ICT Risk Management

ICT risk is a component of the overall risk universe of an enterprise. Other risks Bank or NBFI faces include strategic risk, environmental risk, market risk, credit risk, operational risk, compliance risk, etc. In many enterprises, ICT related risk is considered to be a component of operational risk.

However, even strategic risk can have an ICT component itself, especially where ICT is the key enabler of new business initiatives. The same applies for credit risk, where poor ICT security can lead to lower credit ratings. It is better not to depict ICT risk with a hierarchic dependency on one of the other risk categories.

ICT risk is business risk - specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of ICT within a Bank or NBFI. It consists of ICT related events and conditions that could potentially impact the business. It can occur with both uncertain frequency and magnitude and it creates challenges in meeting strategic goals and objectives.

5.3.1 ICT Risk Governance

i) The Bank or NBFI shall form an ICT Risk Management Committee to govern overall ICT risks and relevant mitigation measures.

ii) The Bank or NBFI shall define the *Risk Appetite* (amount of risk the Bank or NBFI is prepared to accept to achieve its' objectives) in terms of combinations of frequency and magnitude of a risk to absorb loss e.g., financial loss, reputation damage.

iii) The Bank or NBFI shall define the *Risk Tolerance* (tolerable deviation from the level set by the risk appetite definition) having approval from the board/Risk Management Committee and clearly communicated to all stakeholders.

iv) The Bank or NBFI shall review and approve risk appetite and tolerance change over time; especially for new technology, new organizational structure, new business strategy and other factors require the enterprise to reassess its risk portfolio at a regular interval.

v) The Bank or NBFI shall define the risk responsibilities to individuals for ensuring successful completion.

vi) The Bank or NBFI shall define the risk accountability applies to those who owned the required resources and have the authority to approve the execution and/or accept the outcome of an activity within specific ICT Risk processes. Ownership of risk stays with owner or custodian whoever is in better position to mitigate the identified risk for that specific ICT asset.

vii) The Bank or NBFI shall acknowledge all risks by *Risk Awareness* so that those are well understood and known and recognized as the means to manage them.

viii) The Bank or NBFI shall contribute to executive management's understanding of the actual exposure to ICT risk by *Open Communication,* enabling definition of appropriate and informed risk responses.

ix) The Bank or NBFI shall aware amongst all internal stakeholders of the importance of integrating risk and opportunity in their daily duties.

x) The Bank or NBFI shall be transparent to external stakeholders regarding the actual level of risk and risk management processes in use.

xi) The Bank or NBFI shall begin *Risk-aware Culture* from the top with board and executives, who set direction, communicate risk-aware decision making and reward effective risk management behaviors.

xii) ICT security department/unit/cell shall report status of identified ICT security risk to the ICT security committee and Risk Management Committee periodically as defined in the policy.

5.3.2 ICT Risk Assessment

Meaningful ICT risk assessments and risk-based decisions require ICT risks to be expressed in unambiguous and clear, business-relevant terms. Effective risk management requires mutual understanding between ICT and the business over which risk needs to be managed. All stakeholders must have the ability to understand and express how adverse events may affect business objectives. An ICT person shall understand how ICT-related failures or events can impact enterprise objectives and cause direct or indirect loss to the enterprise. A business person shall understand how ICT-related failures or events can affect key services and processes.

i) The Bank or NBFI shall establish business impact analysis needs to understand the effects of adverse events. Bank or NBFI may practice several techniques and options that can help them to describe ICT risks in business terms.

ii) The Bank or NBFI shall practice the development and use of *Risk Scenarios* technique to identify the important and relevant risks amongst all. The developed risk scenarios can be used during risk analysis where frequency and impact of the scenario are assessed.

iii) The Bank or NBFI shall define *Risk Factors* those influence the frequency and/or business impact of risk scenarios.

iv) The Bank or NBFI shall interpret risk factors as casual factors of the scenario that is materializing, or as vulnerabilities or weaknesses.

v) ICT security department/unit/cell shall conduct periodic ICT risk assessment of ICT related assets (process and system) and provide recommendation to risk owners for mitigation.

5.3.3 ICT Risk Response

Risk response is to bring measured risk in line with the defined risk tolerance level for the organization. In other words, a response needs to be defined such that as much future residual risk as possible (usually depending on budgets available) falls within risk tolerance limits. When the analysis shows risks deviating from the defined tolerance levels, a response needs to be defined. This response can be any of the four possible ways such as Risk Avoidance, Risk Reduction/Mitigation, Risk Sharing/Transfer and Risk Acceptance.

i) The Bank or NBFI shall develop a set of metrics to serve as risk indicators. Indicators for risks with high business impact are most likely to be *Key Risk Indicators (KRIs).*

ii) The Bank or NBFI shall give effort to implement, measure and report different indicators that are equivalent in sensitivity.

iii) Selection of the right set of KRIs, Bank or NBFI shall carry out:

a) Provide an early warning for a high risk to take proactive action

b) Provide a backward-looking view on risk events that have occurred

c) Enable the documentation and analysis of trends

d) Provide an indication of the risk's appetite and tolerance through metric setting

e) Increase the likelihood of achieving the strategic objectives

f) Assist in continually optimizing the risk governance and management environment

iv) The Bank or NBFI shall define risk response to bring risk in line with the defined risk appetite for the Bank or NBFI after risk analysis.

v) The Bank or NBFI shall strengthen overall ICT risk management practices with sufficient risk management processes.

vi) The Bank or NBFI shall introduce a number of control measures intended to reduce either of an adverse event and/or the business impact of an event.

vii) The Bank or NBFI shall share or reduce risk frequency or impact by transferring or otherwise sharing a portion of the risk, e.g. insurance, outsourcing.

5.4. ICT Service Delivery Management

ICT Service Management covers the dynamics of technology operation management that includes capacity management, request management, change management, incident and problem

management etc. The objective is to set controls to achieve the highest level of ICT service quality by minimum operational risk.

5.4.1 Change Management

i) Changes to information processing facilities and systems shall be controlled.

ii) Bank or NBFI shall prepare Business Requirement Document (BRD) which will cover the requirements of system changes and the impact that will have on business processes, security matrix, reporting, interfaces, etc.

iii) All changes of business application implemented in the production environment must be governed by a formal documented process with necessary change details.

iv) Audit trails shall be maintained for business applications.

v) Bank or NBFI shall prepare rollback plan for unexpected situation.

vi) User Acceptance Test (UAT) for changes and upgrades in application shall be carried out before deployment.

vii) User Verification Test (UVT) for post deployment may be carried out.

5.4.2 Incident Management

An incident occurs when there is an unexpected disruption to the standard delivery of ICT services. The Bank or NBFI shall appropriately manage such incidents to avoid a situation of mishandling that result in a prolonged disruption of ICT services.

i) The Bank or NBFI shall establish an incident management framework with the objective of restoring normal ICT service as quickly as possible following the incident with minimal impact to the business operations. The Bank or NBFI shall also establish roles and responsibilities of staff involved in the incident management process, which includes recording, analyzing, remediating and monitoring incidents.

ii) It is important that incidents are accorded with the appropriate severity level. As part of incident analysis, the Bank or NBFI may delegate the function of determining and assigning incident severity levels to a technical helpdesk function. The Bank or NBFI shall train helpdesk staff to determine incidents of high severity level. In addition, criteria used for assessing severity levels of incidents shall be established and documented.

iii) The Bank or NBFI shall establish corresponding escalation and resolution procedures where the resolution timeframe is proportionate with the severity level of the incident.

iv) The predetermined escalation and response plan for security incidents shall be tested on a periodic basis.

v) The Bank or NBFI shall form an *ICT Emergency Response Team*, comprising staff within the Bank or NBFI with necessary technical and operational skills to handle major incidents.

vi) In some situations, major incidents may further develop adversely into a crisis. Senior management shall be kept apprised of the development of these incidents so that the decision to activate the disaster recovery plan can be made on a timely basis. Bank or NBFI shall inform Bangladesh Bank as soon as possible in the event that a critical system has failed over to its disaster recovery system.

vii) The Bank or NBFI shall keep customers informed of any major incident. Being able to maintain customer confidence throughout a crisis or an emergency situation is of great importance to the reputation and soundness of the Bank or NBFI.

viii) As incidents may trail from numerous factors, Bank or NBFI shall perform a root-cause and impact analysis for major incidents which result in severe disruption of ICT services. The Bank or NBFI shall take remediation actions to prevent the recurrence of similar incidents.

ix) The root-cause and impact analysis report shall cover following areas:

a) Root Cause Analysis

i. When did it happen?

ii. Where did it happen?

iii. Why and how did the incident happen?

iv. How often had a similar incident occurred over last 2 years?

v. What lessons were learnt from this incident?

b) Impact Analysis

i. Extent of the incident including information on the systems, resources, customers that were affected;

ii. Magnitude of the incident including foregone revenue, losses, costs, investments, number of customers affected, implications, consequences to reputation and confidence;

iii. Breach of regulatory requirements and conditions as a result of the incident.

c) Corrective and Preventive Measures

i. Immediate corrective action to be taken to address consequences of the incident. Priority shall be placed on addressing customers' concerns.

ii. Measures to address the root cause of the incident.

iii. Measures to prevent similar or related incidents from occurring. 4.2.10 The Bank or NBFI shall adequately address all incidents within corresponding resolution timeframes and monitor all incidents to their resolution.

5.4.3 Problem Management

While the objective of incident management is to restore the ICT service as soon as possible, the aim of problem management is to determine and eliminate the root cause to prevent the occurrence of repeated incidents.

i) Bank or NBFI shall establish a process to log the information system related problems.

ii) The Bank or NBFI shall have the process of workflow to escalate any problem to a concerned person to get a quick, effective and orderly response.

iii) Problem findings and action steps taken during the problem resolution process shall be documented.

iv) A trend analysis of past problems shall be performed to facilitate the identification and prevention of similar problems.

5.4.4 Capacity Management

The goal of capacity management is to ensure that ICT capacity meets current and future business requirements in a cost-effective manner.

i) To ensure that ICT systems and infrastructure are able to support business functions, the Bank or NBFI shall ensure that indicators such as performance, capacity and utilization are monitored and reviewed.

ii) The Bank or NBFI shall establish monitoring processes and implement appropriate thresholds to plan and determine additional resources to meet operational and business requirements effectively.

5.5. Infrastructure Security Management

The ICT landscape is vulnerable to various forms of attacks. The frequency and malignancy of such attacks are increasing. It is imperative that Bank or NBFI implements security solutions at the data, application, database, operating systems and networks to adequately address related threats. Appropriate measures shall be implemented to protect sensitive or confidential information such as customer personal information, account and transaction data which are stored and processed in systems. Customers shall be properly authenticated before access to online transactions, sensitive personal or account information.

5.5.1 Asset Management

i) Prior to procuring any new ICT assets, compatibility assessment (with existing system) shall be performed by the Bank or NBFI.

ii) All ICT asset procurement shall be complied with the procurement policy of Bank or NBFI.

iii) Each ICT asset shall be assigned to a custodian (an individual or entity) who will be responsible for the development, maintenance, usage, security and integrity of that asset.

iv) All ICT assets shall be clearly identified and labeled. Labeling shall reflect the established classification of assets.

v) Bank or NBFI shall maintain an ICT asset inventory stating significant details (e.g. owner, custodian, purchase date, location, license number, configuration, etc.).

vi) Bank or NBFI shall review and update the ICT asset inventory periodically.

vii) Information system assets shall be adequately protected from unauthorized access, misuse or fraudulent modification, insertion, deletion, substitution, suppression or disclosure.

viii) The Bank or NBFI shall establish a *Disposal Policy* for information system asset protection. All data on equipment and associated storage media must be destroyed or overwritten before sale, disposal or re-issue.

ix) Bank or NBFI shall provide guidelines for the use of portable devices, especially for the usage at outside premises.

x) Bank or NBFI shall provide policy to return back organizational assets from employees/external parties upon termination of their employment, contract or agreement.

xi) Bank or NBFI shall comply with the terms of all software licenses and shall not use any software that has not been legally purchased or otherwise legitimately obtained.

xii) Outsourced software used in production environment shall be subjected to support agreement with the vendor.

xiii) Bank or NBFI shall approve list of Software which will only be used in any computer.

xiv) Use of unauthorized or pirated software must strictly be prohibited throughout the Bank or NBFI.

5.5.2 Desktop/Laptop Devices Controls

i) Desktop computers shall be connected to UPS to prevent damage of data and hardware.

ii) Before leaving a desktop or laptop computer unattended, users shall apply the "*Lock Workstation*" feature. If not applied then the device will be automatically locked as per policy of Bank or NBFI.

iii) Confidential or sensitive information that stored in laptops must be encrypted.

iv) Desktop computers, laptops, monitors, etc. shall be turned off at the end of each workday.

v) Laptops, computer media and any other forms of removable storage containing sensitive information (e.g. CD ROMs, Zip disks, PDAs, Flash drives, external hard-drives) shall be stored in a secured location or locked cabinet when not in use.

vi) Access to USB port for Desktop/Laptop computers shall be controlled.

vii) Other information storage media containing confidential data such as paper, files, tapes, etc. shall be stored in a secured location or locked cabinet when not in use.

viii) Individual users must not install or download software applications and/or executable files to any desktop or laptop computer without prior authorization.

ix) Desktop and laptop computer users shall not write, compile, copy, knowingly propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer system (e.g. virus, worm, Trojan etc).

x) Any kind of viruses shall be reported immediately.

xi) Viruses shall not be cleaned/ deleted without expert assistance unless otherwise instructed.

xii) User identification (ID) and authentication (password) shall be required to access all desktops and laptops whenever turned on or restarted.

xiii) Standard virus detection software must be installed on all desktop and laptop computers and shall be configured to check files when read and routinely scan the system for viruses.

xiv) Desktop and laptop computers shall be configured to log all significant computer security relevant events. (e.g. password guessing, unauthorized access attempts or modifications to applications or systems software.)

xv) All computers shall be placed above the floor level and away from windows.

5.5.3 BYOD Controls

“Bring Your Own Device” (BYOD) is a relatively new practice adopted by banks and financial institutions to enable their employees to access corporate email, calendars, applications and data from their personal mobile devices like smart phones, tablet computers, etc. Bank or NBFI shall be aware of the heightened security risks associated with BYOD due to challenges in securing, monitoring and controlling employees’ personal devices.

i) Bank or NBFI shall conduct a comprehensive risk assessment on the BYOD implementation to ensure that measures adopted sufficiently to mitigate the security risks associated with BYOD.

ii) Bank or NBFI shall not proceed with the BYOD implementation if they are unable to adequately manage the associated security risks.

iii) BYOD is associated with a number of information security risks such as:

a) Loss, disclosure or corruption of corporate data on Personally Owned Devices (PODs);

b) Incidents involving threats to, or compromise of, the ICT infrastructure and other information assets (e.g. malware infection or hacking) of Bank or NBFI;

c) Noncompliance with applicable laws, regulations and obligations (e.g. privacy or piracy);

d) Intellectual property rights for information created, stored, processed or communicated on PODs in the course of work for the Bank or NBFI.

Due to information security risks associated with BYOD, employees who wish to opt-in to BYOD must be authorized to do so and must not introduce unacceptable risks onto the banks' networks by failing to secure their own equipment.

iv) The Bank or NBFI may implement appropriate forms of device authentication for PODs approved by authority, such as digital certificates created for each specific device.

v) The Bank or NBFI has the right to control its information. This must include the right to backup, retrieve, modify, determine access and/or delete bank data without reference to the owner or user of the POD.

vi) Any POD used to access, store or process sensitive information must encrypt data transferred over the network (e.g. using SSL or a VPN).

vii) The employee's device shall be remotely wiped if the device is lost, or the employee terminates his/her employment, or ICT detects a data or policy breach, a virus or similar threat to the security of the bank's data and technology infrastructure.

5.5.4 Server Security Controls

i) Users shall have specific authorization for accessing servers with defined set of privileges.

ii) Additional authentication mechanism shall be used to control access of remote users.

iii) Inactive session shall be expired after a defined period of inactivity.

iv) Activities of System Administrators shall be logged. Servers containing sensitive and confidential data may export activity logs to a central log host.

v) Bank or NBFI shall maintain test server(s) to provide a platform for testing of configuration settings, new patches and service packs before applied on the production system.

vi) Bank or NBFI shall ensure the security of file sharing process. File and print shares must be disabled if not required or kept at a minimum where possible.

vii) All unnecessary services running in the production server shall be disabled. Any new services shall not run in production server without prior testing.

viii) All unnecessary programs shall be uninstalled from production servers.

ix) In case of virtualization:

a) Bank or NBFI shall plan of setting limit on the use of resources (e.g., processors, memory, disk space, virtual network interfaces) by each VM.

b) Host and guest Operating System (OS) must be updated with new/required security patches and other patches if necessary. Patching requirements shall also be applied to the virtualization software.

c) Like physical servers, virtual servers need to be backed up regularly.

d) Bank or NBFI shall ensure that host and guests use synchronized time**.**

e) File sharing shall not be allowed between host and guest OSs, if not required.

5.5.5 Data Center Controls

As critical systems and data of a Bank or NBFI are concentrated and housed in the Data Center (DC), it is important that the DC is resilient and physically secured from internal and external threats.

5.5.5.1 Physical Security

i) Physical security shall be applied to the information processing area or Data Center. DC must be a restricted area and unauthorized access shall be strictly prohibited. 5.5.1.2 The Bank or NBFI shall limit access to DC to authorized staff only. The Bank or NBFI shall only grant access to the DC on a need to have basis. Physical access of staff to the DC shall be revoked immediately if it is no longer required.

ii) Access authorization procedures shall be strictly applied to vendors, service providers, support staff and cleaning crews. The Bank or NBFI shall ensure that visitors are accompanied at all times by an authorized employee while in the DC.

iii) Access authorization list shall be maintained and reviewed periodically for the authorized person to access the Data Center.

iv) All physical access to sensitive areas must be logged with purpose of access into the Data Center.

v) The Bank or NBFI shall ensure that the perimeter of the DC, facility and equipment room are physically secured and monitored. The Bank or NBFI shall employ physical, human and procedural controls for 24 hours such as the use of security guards, card access system, mantraps and surveillance system where appropriate.

vi) Emergency exit door shall be available.

vii) Data Center must have a designated custodian or manager in charge to provide authorization and to ensure compliance with Policy.

viii) An inventory of all computing equipment, associated equipment and consumables housed in DC must be maintained by the manager or a delegate.

ix) Where DC is operated by an outsourced service supplier, the contract between the bank and supplier must indicate that all the requirements of Policy regarding physical security must be complied with and that the Bank or NBFI reserves the right to review physical security status at any time.

x) Where DC is operated by an outsourced service supplier, the responsibility for physical security lies with the supplier, but access to such facilities dedicated to bank use must be reviewed and authorized by the Bank or NBFI.

xi) The physical security of Data Center premises shall be reviewed at least once each year.

5.5.5.2 Environmental Security

i) Protection of Data Center from the risk of damage due to fire, flood, explosion and other forms of disaster shall be designed and applied. To build Data Center and Disaster Recovery Site in multi-tenant facilitated building is discouraged.

ii) Layout design of Data Center including power supply and network connectivity shall be properly documented.

iii) Development and test environment shall be separated from production.

iv) Separate channels for data and power cables to protect from interception or any sort of damages shall be made in the data center.

v) Water detection devices shall be placed below the raised floor, if it is raised.

vi) Any accessories or devices not associated with Data Center and powered off devices shall not be allowed to store in the Data Center. Separate store room must be in place to keep all sorts of unused and redundant IT equipments.

vii) Closed Circuit Television (CCTV) camera shall be installed at appropriate positions of all sides for proper monitoring.

viii) The sign of "No eating, drinking or smoking" shall be in display.

ix) Dedicated office vehicles for any of the emergencies shall always be available on-site. Availing of public transport must be avoided while carrying critical equipments outside the bank’s premises to avoid the risk of any causality.

x) Data Center shall have dedicated telephone communication.

xi) Address and telephone or mobile numbers of all contact persons (e.g. fire service, police station, service providers, vendors and all ICT personnel) must be available to meet any emergency necessity.

xii) Power supply system and other support units must be separated from production site and placed in secure area to reduce the risks from environmental threats.

viii) Power supply from source (Main Distribution Board or Generator) to Data Center must be dedicated. Electrical outlets from these power sources for any other devices must be restricted and monitored to avoid the risk of overloading.

ix) The following environmental controls shall be installed:

a) Uninterrupted Power Supply (UPS) with backup units

b) Backup Power Supply

c) Temperature and humidity measuring devices

d) Water leakage precautions and water drainage system from Air Conditioner

e) Air conditioners with backup units. Industry standard air conditioning system shall be in place to avoid water leakage from the conventional air conditioning system.

f) Emergency power cut-off switches where applicable

g) Emergency lighting arrangement

h) Dehumidifier for humidity control 5.5.2.15 The above mentioned environmental controls shall be regularly tested and maintenance service contract shall be for 24x7 bases.

5.5.5.3 Fire Prevention

i) Ceiling and door of Data Center shall be fire-resistant.

ii) Fire suppression equipment shall be installed and tested periodically.

iii) Automatic fire/smoke alarming system shall be installed and tested periodically.

iv) There shall be fire detector below the raised floor, if it is raised.

v) Electric cables and data cables in the Data Center must maintain quality and be concealed.

vi) Flammable items such as paper, wooden items, plastics, etc. shall not be allowed to store in the Data Center.

5.5.6 Server/Network Room/Rack Controls

i) Server/network room/rack must have a glass enclosure with lock and key under a responsible person.

ii) Physical access shall be restricted, visitors log must exist and to be maintained for the server room.

iii) Access authorization list must be maintained and reviewed on regular basis.

iv) There shall be a provision to replace the server and network devices within shortest possible time in case of any disaster.

v) Server/network room/rack shall be air-conditioned. Water leakage precautions and water drainage system from Air Conditioner shall be installed.

vi) Power generator shall be in place to continue operations in case of power failure.

vii) UPS shall be in place to provide uninterrupted power supply to the server and required devices.

viii) Proper attention must be given on overloading electrical outlets with too many devices.

ix) Channel alongside the wall shall be prepared to allow all required cabling in neat and safe position as per layout of power supply and data cables.

x) Address and phone numbers of all contact persons (e.g. fire service, police station, service providers, vendors and all ICT/ responsible personnel) must be available to cope with any emergency situation.

xi) Power supply shall be switched off before leaving the server room if otherwise not required.

xii) Fire extinguisher shall be placed outdoor visible area of the server room. This must be maintained and checked on an annual basis.

5.5.7 Networks Security Management

i) The Bank or NBFI shall establish baseline standards to ensure security for Operating Systems, Databases, Network equipments and portable devices which shall meet organization's policy.

ii) The Bank or NBFI shall conduct regular enforcement checks to ensure that the baseline standards are applied uniformly and non-compliances are detected and raised for investigation.

iii) The Network Design and its security configurations shall be implemented under a documented plan. There shall have different security zones defined in the network design.

iv) All type of cables including UTP, fiber, power shall have proper labeling for further corrective or preventive maintenance works.

v) The Bank or NBFI shall ensure physical security of all network equipments.

vi) Groups of information services, users and information systems shall be segregated in networks, e.g. VLAN.

vii) Unauthorized access and electronic tampering shall be controlled strictly. Mechanism shall be in place to encrypt and decrypt sensitive data travelling through WAN or public network.

viii) The Bank or NBFI shall install network security devices, such as firewalls as well as intrusion detection and prevention systems, at critical stages of its ICT infrastructure to protect the network perimeters.

ix) The Bank or NBFI shall deploy firewalls, or other similar measures, within internal networks to minimize the impact of security exposures originating from third party or overseas systems, as well as from the internal trusted network.

x) Secure Login feature (i.e. SSH) shall be enabled in network devices for remote administration purposes. Any unencrypted login option (i.e. TELNET) shall be disabled.

xi) The Bank or NBFI shall backup and review rules on network security devices on a regular basis to determine that such rules are appropriate and relevant.

xii) The Bank or NBFI shall establish redundant communication links for WAN connectivity.

xiii) The Bank or NBFI deploying Wireless Local Area Networks (WLAN) within the organization shall be aware of risks associated in this environment. Secure communication protocols for transmissions between access points and wireless clients shall be implemented to secure the corporate network from unauthorized access.

xiv) SYSLOG Server may be established depending on Network Size to monitor the logs generated by network devices.

xv) Authentication Authorization and Accounting (AAA) Server may be established depending on Network Size to manage the network devices effectively.

xvi) Role-based and/or Time-based Access Control Lists (ACLs) shall be implemented in the routers to control network traffic.

xvii) Real time health monitoring system for infrastructure management may be implemented for surveillance of all network equipments and servers.

xviii) Connection of personal laptop to office network or any personal wireless modem with the office laptop/desktop must be restricted and secured.

xix) The Bank or NBFI shall change all default passwords of network devices.

xx) All unused ports of access switch shall be shut-off by default if otherwise not defined.

xxi) All communication devices shall be uniquely identifiable with proper authentication.

xxii) Role-based administration shall be ensured for the servers.

5.5.8 Internet Access Management

i) Internet access shall be provided to employees according to the approved Internet Access Management Policy.

ii) Access to and use of the internet from bank premises must be secure and must not compromise information security of Bank or NBFI.

iii) Access to the Internet from bank premises and systems must be routed through secure gateways.

iv) Any local connection directly to the Internet from Bank or NBFI premises or systems, including standalone PCs and laptops, is prohibited unless approved by Information Security.

v) Employees shall be prohibited from establishing their own connection to the Internet using banks' systems or premises.

vi) Use of locally attached modems with banks' systems in order to establish a connection with the Internet or any third-party or public network via broadband, ISDN or PSTN services is prohibited unless specifically approved.

vii) Internet access provided by the Bank or NBFI must not be used to transact any commercial business activity that is not done by the Bank or NBFI. Personal business interests of staff or other personnel must not be conducted.

viii) Internet access provided by the Bank or NBFI must not be used to engage in any activity that knowingly contravenes any criminal or civil law or act. Any such activity will result in disciplinary action of the personnel involved.

ix) All applications and systems that require connections to the Internet or third-party and public networks must undergo a formal risk analysis during development and before production use and all required security mechanisms must be implemented.

5.5.9. Email Management

i) Email system shall be used according to the Bank's or NBFI's policy.

ii) Access to email system shall only be obtained through official request.

iii) Email shall not be used to communicate confidential information to external parties unless encrypted using approved encryption facilities.

iv) Employees must consider the confidentiality and sensitivity of all email content, before forwarding email or replying to external parties.

v) Information transmitted by email must not be defamatory, abusive, involve any form of racial or sexual abuse, damage the reputation of the Bank or NBFI, or contain any material that is harmful to employees, customers, competitors, or others. The willful transmission of any such material is likely to result in disciplinary action.

vi) Bank email system is principally provided for business purposes. Personal use of the bank email system is only allowed under management discretion and requires proper permission; such personal use may be withdrawn or restricted at any time.

vii) Corporate email address must not be used for any social networking, blogs, groups, forums, etc. unless having management approval.

viii) Email transmissions from the Bank or NBFI must have a disclaimer stating about confidentiality of the email content and asking intended recipient.

ix) Concerned department shall perform regular review and monitoring of email services.

5.6. Access Control of Information System

The Bank or NBFI shall only grant access rights and system privileges based on job responsibility. The Bank or NBFI shall check that no person by virtue of rank or position shall have any intrinsic right to access confidential data, applications, system resources or facilities for legitimate purposes.

5.6.1 User Access Management

i) The Bank or NBFI shall only grant user access to ICT systems and networks on a need-to-use basis and within the period when the access is required.

ii) The Bank or NBFI shall closely monitor non-employees (contractual, outsourced, or vendor staff) for access restrictions.

iii) Each user must have a unique User ID and a valid password.

iv) User ID Maintenance form with access privileges shall be duly approved by the appropriate authority.

v) User access shall be locked for unsuccessful login attempts.

vi) User access privileges must be kept updated for job status changes.

vii) The Bank or NBFI shall ensure that records of user access are uniquely identified and logged for audit and review purposes.

viii) The Bank or NBFI shall perform regular reviews of user access privileges to verify that privileges are granted appropriately.

5.6.2 Password Management

i) The Bank or NBFI shall enforce strong password controls over users' access.

ii) Password controls shall include a change of password upon first logon.

iii) Password definition parameters shall ensure that minimum password length is maintained according to Bank's Policy (at least 6 characters).

iv) Password shall be combination of at least three of stated criteria like uppercase, lowercase, special characters and numbers.

v) Maximum validity period of password shall not be beyond the number of days permitted in the Bank's Policy (maximum 90 days cycle).

vi) Parameter to control maximum number of invalid logon attempts shall be specified properly in the system according to the Bank's Policy (maximum 3 consecutive times).

vii) Password history maintenance shall be enabled in the system to allow same passwords to be used again after at least three (3) times.

viii) Administrative passwords of Operating System, Database and Business Applications shall be kept in a safe custody with sealed envelope.

5.7. Business Continuity and Disaster Recovery Management

Business Continuity and Disaster Recovery Management is required for planning of business resiliency for critical incidents, operational risks take into account for wide area disasters, Data Center disasters and the recovery plan. The primary objective of Business Continuity Plan (BCP) is to enable a Bank or NBFI to survive in a disaster and to re-establish normal business operations. In order to survive with minimum financial and reputational loss, Bank or NBFI shall assure that critical operations can resume normal processing within a reasonable time frame. The contingency plan shall cover the business resumption planning and disaster recovery planning. Contingency plan shall also address the backup, recovery and restore process.

5.7.1 Business Continuity Plan (BCP)

i) Bank or NBFI must have an approved Business Continuity Plan addressing the recovery from disaster to continue its operation.

ii) Approved BCP shall be circulated to all relevant stakeholders. The recipients would receive a copy of amended plan whenever any amendment or alteration takes place.

iii) Documents related to BCP must be kept in a secured off-site location. One copy shall be stored in the office for ready reference.

iv) The BCP shall be coordinated with and supported by the Business Impact Analysis (BIA) and the Disaster Recovery Plan (DRP) considering system requirements, processes and interdependencies.

v) BCP shall address the followings:

a) Action plan to restore business operations within the specified time frame for: i) office hour disaster ii) outside office hour disaster.

b) Emergency contacts, addresses and phone numbers of employees, venders and agencies.

c) Grab list of items such as backup tapes, laptops, flash drives, etc.

d) Disaster recovery site map 7.1.6 BCP must be tested and reviewed at least once a year to ensure the effectiveness.

5.7.2. Disaster Recovery Plan (DRP)

i) Bank or NBFI must have an approved Disaster Recovery Plan. In formulating and constructing a rapid recovery plan, the Bank or NBFI shall include a scenario analysis to identify and address various types of contingency scenarios. The Bank or NBFI shall consider scenarios such as major system outages which may be caused by system faults, hardware malfunction, operating errors or security incidents as well as a total incapacitation of the primary DC.

ii) The Bank or NBFI shall establish a Disaster Recovery Site (DRS) which is geographically separated from the primary site (minimum of 10 kilometers radial distance but choice of different

seismic zone will be preferred) to enable the restoration of critical systems and resumption of business operations when a disruption occurs at the primary site.

iii) If Disaster Recovery Site (DRS) is not in different seismic zone, Bank or NBFI may establish a third site in different seismic zone which will be treated as Disaster Recovery Site (DRS)/Far DC. In such case the DRS in near location will be treated as Near DC and shall be configured accordingly.

iv) DRS and/or Near DC shall be equipped with compatible hardware and telecommunication equipment to support the critical services of the business operation in the event of a disaster.

v) Physical and environmental security of the DRS and/or Near DC shall be maintained.

vi) The Bank or NBFI shall define system recovery and business resumption priorities and establish specific recovery objectives including recovery time objective (RTO) and recovery point objective (RPO) for ICT systems and applications. RTO is the duration of time, from the point of disruption, within which a system shall be restored. RPO refers to the acceptable amount of data loss for an ICT system while a disaster occurs.

vii) The Bank or NBFI shall consider inter-dependencies between critical systems in drawing up its recovery plan and conducting contingency tests.

viii) The Bank or NBFI may explore recovery strategies and technologies such as on-site redundancy and real-time data replication to enhance the bank's recovery capability.

ix) Information security shall be maintained properly throughout the recovery process.

x) An up-to-date and tested copy of the DR plan shall be securely held off-site. One copy shall be stored in the office for ready reference.

xi) The Bank or NBFI shall test and validate at least annually the effectiveness of recovery requirements and the ability of staff to execute the necessary emergency and recovery procedures.

xii) The Bank or NBFI shall involve its business users in the design and execution of comprehensive test cases to verify that recovered systems function properly.

xiii) DR test documentation shall include at a minimum of Scope, Plan and Test Result. Test report shall be communicated to management and other stakeholders and preserved for future necessity.

5.7.3 Data Backup and Restore Management

i) The Bank or NBFI shall develop a data backup and recovery policy. Each business application must have a planned, scheduled and documented backup strategy, involving the making of both on- and off-line backups and the transfer of backups to secure off-site storage.

ii) Details of the planned backup schedule for each business application must be created in line with the classification of the application and the information it supports and must specify the

type of back-up required (full, partial, incremental, differential, real-time monitoring) at each point in the back-up schedule.

iii) The frequency of backups taken for information must be determined in line with the classification of the information and the requirements of the business continuity plans for each application.

iv) The details of the planned backup schedule for each business application must include the retention period for backed-up or archived information and the retention period must be consistent with local legal and regulatory requirements.

v) All media contained backed-up information must be labeled with the information content, backup cycle, backup serial identifier, backup date and classification of the information content.

vi) The backup inventory and log sheet shall be maintained, checked and signed by the supervisor.

vii) The Bank or NBFI shall encrypt backup data in tapes or disks, containing sensitive or confidential information, before transported offsite for storage.

viii) At least one copy of backup shall be kept on-site for the time critical delivery.

ix) The process of restoring information from both on- and off-site backup storage must be documented.

x) The Bank or NBFI shall carry out periodic testing and validation of the recovery capability of backup media and assess whether it is adequate and sufficiently effective to support the bank's recovery process.

5.8. Acquisition and Development of Information Systems

For any new application of business function for the Bank or NBFI requires rigorous analysis before acquisition or development to ensure that business requirements are met in an effective and efficient manner. This process covers the definition of needs, consideration of alternative sources, review of technological and economic feasibility, execution of risk analysis and cost-benefit analysis and conclusion of a final decision to 'make' or 'buy'.

Many systems fail because of poor system design and implementation, as well as inadequate testing. The Bank or NBFI shall identify system deficiencies and defects at the system design, development and testing phases. The Bank or NBFI shall establish a steering committee, consisting of business owners, the development/technical team and other stakeholders to provide oversight and monitoring of the progress of the project, including deliverables to be realized at each phase of the project and milestones to be reached according to the project timetable.

5.8.1 ICT Project Management

i) In drawing up a project management framework, the Bank or NBFI shall ensure that tasks and processes for developing or acquiring new systems include project risk assessment and

classification, critical success factors for each project phase, definition of project milestones and deliverables. The Bank or NBFI shall clearly define in the project management framework, the roles and responsibilities of staff involved in the project.

ii) Project plan for all ICT projects shall be clearly documented and approved. In the project plans, the Bank or NBFI shall set out clearly the deliverables to be realized at each phase of the project as well as milestones to be reached.

iii) The Bank or NBFI shall ensure that user functional requirements, business cases, cost-benefit analysis, systems design, technical specifications, test plans and service performance expectation are approved by the relevant business units and ICT management.

iv) The Bank or NBFI shall establish management oversight of the project to ensure that milestones are reached and deliverables are realized in a timely manner.

5.8.2. Vendor Selection for System Acquisition

i) There must be a core team comprising of personnel from Functional Departments, ICT Department and Internal Control and Compliance Department for vendor selection.

ii) Vendor selection process must have conformity with the Procurement Policy of the Bank or NBFI.

iii) Vendor selection criteria for application must address followings:

a) Market presence

b) Years in operation

c) Technology alliances

d) Extent of customization and work around solutions

e) Financial strength

f) Performance and Scalability

g) Number of installations

h) Existing customer reference

i) Support arrangement

j) Local support arrangement for foreign vendors

k) Weight of financial and technical proposal

5.8.3 In-house Software Development

i) Detailed business requirements shall be documented and approved by the competent authority.

ii) Detailed technical requirements and design shall be prepared.

iii) Application security and availability requirements shall be addressed.

iv) Developed functionality in the application shall be in accordance with design specification and documentation.

v) Software Development Life Cycle (SDLC) with User Acceptance Test (UAT) shall be followed and conducted in the development and implementation stage.

vi) User Verification Test (UVT) for post deployment shall be carried out.

vii) System documentation and User Manual shall be prepared and handed over to the concerned department.

viii) Source code must be available with the concerned department and kept secured.

ix) Source code shall contain title area with author name, date of creation, last date of modification and other relevant information.

x) Application shall be in compliance with relevant controls of Bank's ICT Security Policy.

xi) Necessary '*Regulatory Compliance*' requirements must be taken into account by the Bank or NBFI.

5.9. Alternative Delivery Channels (ADC) Security Management

"Channelize through channels" is the new paradigm for banking today, which in earlier relied solely on the branch network. Branchless banking is a distribution channel strategy used for delivering financial services without relying on bank branches. Alternate Delivery Channels are methods for providing banking services directly to the customers. Customers can perform banking transactions through their ATM, contact the bank's Call Center for any inquiry, access the digital Interactive Voice Response (IVR), perform transactions through Internet Banking and even on phones through mobile banking, etc. These channels have enabled banks to reach a wide consumer-base regardless of time and geographic location. ADCs ensure higher customer satisfaction at lower operational expenses and transaction costs.

5.9.1 ATM/POS Transactions

The ATMs and Point-of-Sale (POS) devices have facilitated cardholders with the convenience of withdrawing cash as well as making payments to merchants and billing organizations. However, these systems are targets where card skimming attacks are perpetrated. To secure consumer confidence in using these systems, the Bank or NBFI shall consider putting in place the following measures to counteract fraudsters' attacks on ATMs and POS devices:

i) The Bank or NBFI shall install anti-skimming solutions on ATM devices to detect the presence of unknown devices placed over or near a card entry slot.

ii) The Bank or NBFI shall install detection mechanisms and send alerts to appropriate staff for follow-up response and action.

iii) The Bank or NBFI shall implement tamper-resistant keypads to ensure that customers' PINs are encrypted during transmission.

iv) The Bank or NBFI shall implement appropriate measures to prevent shoulder surfing of customers' PINs.

v) The Bank or NBFI may implement biometric finger vein sensing technology to resist PIN compromise.

vi) The Bank or NBFI shall conduct video surveillance of activities for 24 hours at these machines and maintain the quality of CCTV footage and preserve for at least one year.

vii) The Bank or NBFI shall introduce a centralized online monitoring system for Cash Balance, Loading-Unloading functions, Disorders of machine, etc.

viii) The Bank or NBFI shall deploy security personnel for all ATM devices 24 hour basis.

ix) The Bank or NBFI shall verify that adequate physical security measures are implemented in ATM devices.

x) Bank or NBFI shall inspect all ATM/POS devices frequently to ensure standard practice (i.e., environmental security for ATM, anti-skimming devices for ATM, POS device surface tempering, etc.) is in place with necessary compliance. Inspection log sheet shall be maintained in ATM booth premises and centrally.

xi) Bank or NBFI shall monitor third party cash replenishment vendors' activities constantly and visit third party cash sorting houses regularly.

xii) The Bank or NBFI shall train and provide necessary manual to its merchants about security practices (e.g. signature verification, device tampering/ replacement attempt, changing default password, etc.) to be followed for POS device handling.

xiii) The Bank or NBFI shall educate its customers on security measures that are put in place by the Bank or NBFI and are to maintain by the customers for ATM and POS transactions.

5.9.2 Internet Banking

Information involved in internet banking facility passing over public networks shall be protected from fraudulent activity, dispute and unauthorized disclosure or modification. Banks' internet systems may be vulnerable as financial services are increasingly being provided via the internet. As a counter-measure, the Bank or NBFI shall devise a security strategy and put in place measures to ensure the confidentiality, integrity and availability of its data and systems.

i) The Bank or NBFI shall provide assurance to its customers and users so that online access and transactions performed over the internet are adequately protected and authenticated.

ii) Bank or NBFI shall properly evaluate security requirements associated with its internet banking system and adopt mechanisms which are well-established international standards.

iii) The Bank or NBFI shall formulate Internet Banking Security policy considering technology security aspects as well as operational issues.

iv) The Bank or NBFI shall ensure that information processed, stored or transmitted between the bank and its customers is accurate, reliable and complete. The Bank or NBFI shall also implement appropriate processing and transmission controls to protect the integrity of systems and data, e.g. SSL, TLS.

v) The bank shall implement 2-FA (two-factor authentication) for all types of online financial transactions. Hardware/Software based tokenization means will be preferred. The primary objectives of two-factor authentication are to secure the customer authentication process and to protect the integrity of customer account data and transaction details as well as to enhance confidence in online systems.

vi) An online session needs to be automatically terminated after a fixed period of time unless the customer is re-authenticated for the existing session to be maintained.

vii) The Bank or NBFI shall implement monitoring or surveillance systems to follow-up and address subsequently any abnormal system activities, transmission errors or unusual online transactions.

viii) All system accesses, including messages received shall be logged. Security violations (suspected or attempted) shall be reported and followed up. Bank may acquire tools for monitoring systems and networks against intrusions and attacks.

ix) The Bank or NBFI shall maintain high resiliency and availability of online systems and supporting systems (such as interface systems, backend host systems and network equipment). The Bank or NBFI shall put in place measures to plan and track capacity utilization as well as guard against online attacks. These online attacks may include denial-of-service attacks (DoS attack) and distributed denial-of-service attack (DDoS attack).

x) The Bank or NBFI shall take appropriate measures to minimize exposure to other forms of attacks such as middleman attack which is commonly known as a man-in-the-middle attack (MITMA), man-in-the browser attack or man-in-the application attack.

xi) The information security officer or any other assigned person/team shall undertake periodic penetration tests of the system, which may include:

a) Attempting to guess passwords using password-cracking tools

b) Searching for back door traps in the programs

c) Attempting to overload the system using DDoS (Distributed Denial of Service) and DoS (Denial of Service) attacks

d) Checking middleman attacks

e) Checking of commonly known holes in the software, especially the browser and the e-mail software exist

f) Checking the weaknesses of the infrastructure

g) Taking control of ports

h) Cause application crash

i) Injecting malicious codes to application and database servers 9.2.12 The Bank or NBFI shall educate its customers on security measures to protect them in an online environment.

5.9.3 Payment Cards

Payment cards allow cardholders the flexibility to make purchases wherever they are. Cardholders may choose to make purchases by physically presenting these cards for payments at the merchant or they could choose to purchase over the internet, through mail-order or over the telephone. Payment cards also provide cardholders with the convenience of withdrawing cash at automated teller machines ("ATMs").

Payment cards exist in many forms; with magnetic stripe cards posing the highest security risks. Sensitive payment card data stored on magnetic stripe cards is vulnerable to card skimming attacks. Card skimming attacks can happen at various points of the payment card processing, including ATMs, payment kiosks and POS terminals.

i) The Bank or NBFI which provides payment card services shall implement adequate safeguards to protect sensitive payment card data. The Bank or NBFI shall ensure that sensitive card data is encrypted to ensure the confidentiality and integrity of these data in storage and transmission.

ii) The Bank or NBFI shall ensure that the processing of sensitive or confidential information is done in a secure environment.

iii) The Bank or NBFI shall deploy secure chips with multiple payment application supported to store sensitive payment card data. For interoperability reasons, where transactions could only be resulted by using information from the magnetic stripe on a card, the Bank or NBFI shall ensure that adequate controls are implemented to manage these transactions.

iv) The Bank or NBFI shall perform (not a third party payment processing service provider) the authentication of customers' sensitive static information, such as PINs or passwords. The Bank or NBFI shall perform regular security reviews of the infrastructure and processes being used by its service providers.

v) Equipment used to generate payment card PINs and keys shall be managed in a secured manner.

vi) Card personalization, PIN generation, Card distribution, PIN distribution, Card activation groups shall be different from each other.

vii) The Bank or NBFI shall ensure that security controls are implemented at payment card systems and networks. Bank or NBFI must comply with the industry security standards, e.g. - Payment Card Industry Data Security Standard (PCI DSS) to ensure the security of cardholder's data.

viii) The Bank or NBFI shall only activate new payment cards upon obtaining the customer's instruction.

ix) The Bank or NBFI shall implement a dynamic one-time-password ("OTP") as 2-FA for CNP (Card Not Present) transactions via internet to reduce fraud risk associated with it.

x) To enhance card payment security, the Bank or NBFI shall promptly notify cardholders via transaction alerts including source and amount for any transactions made on the customers' payment cards.

xi) The Bank or NBFI shall set out risk management parameters according to risks posed by cardholders, the nature of transactions or other risk factors to enhance fraud detection capabilities.

xii) The Bank or NBFI shall implement solution to follow up on transactions exhibiting behavior which deviates significantly from a cardholder's usual card usage patterns. The Bank or NBFI shall investigate these transactions and obtain the cardholder's authorization prior to completing the transaction.

5.9.4 Mobile Financial Services

Controls over mobile transactions are required to manage the risks of working in an unprotected environment. The Bank or NBFI shall formulate security controls, system availability and recovery capabilities, which commensurate with the level of risk exposure, for operations.

i) Security standards shall be followed appropriate to the complexity of services offered.

ii) Banks or NBFIs shall clearly identify risks associated with the types of services being offered in the risk management process.

iii) Appropriate risk mitigation measures shall be implemented like transaction limit, transaction frequency limit, fraud checks, AML checks etc. depending on the risk perception, unless otherwise mandated by the regulatory body.

iv) Bank or NBFI shall arrange an agreement with Mobile Network Operator (MNOs) about SIM replacement process which includes sending prior notification and getting confirmation to ensure appropriate measures of MFS account for avoiding risk of unwanted transactions.

v) Services provided by banks through mobile shall comply with security principles and practices for the authentication of transactions mandated by the regulatory body.

vi) Bank or NBFI shall conduct periodic risk management analysis and security assessment of the MFS operation and take appropriate measures accordingly.

vii) Bank or NBFI shall have conformity with '*Regulatory Compliance'* requirements of the country.

viii) Proper documentation of security practices, guidelines, methods and procedures used in such mobile financial services shall be maintained and updated.

5.10. Service Provider Management

There is an increasing reliance on external service providers as partners in achieving the growth targets and as effective cost alternatives. ICT outsourcing comes in many forms and permutations. Some of the most common types of ICT outsourcing are in systems development and maintenance, support to DC operations, network administration, disaster recovery services, application hosting and hardware maintenance.

5.10.1 Outsourcing

Now-a-days commercial banks outsource their different ICT services. Agreements of such outsourcing arrangement usually include performance targets, service levels, availability, reliability, scalability, compliance, audit, security, contingency planning, disaster recovery capability and backup processing facility.

i) The board of directors and senior management shall fully understand risks associated with ICT outsourcing. Before appointing a service provider, due diligence shall be carried out to determine its viability, capability, reliability, track record and financial position.

ii) The Bank or NBFI shall ensure that contractual terms and conditions governing the roles, relationships, obligations and responsibilities of all contracting parties are set out fully in written agreements.

iii) Outsourcing activities shall be evaluated based on the following practices:

a) Objective behind Outsourcing

b) Economic viability

c) Risks and security concerns. 10.1.4 ICT outsourcing shall not result in any weakening or degradation of the bank's internal controls. The Bank or NBFI shall require the service provider to employ a high standard of care and diligence in its security policies, procedures and controls to protect the confidentiality and security of its sensitive or confidential information, such as customer data, object programs and source codes.

iv) The Bank or NBFI shall require the service provider to implement security policies, procedures and controls that are at least as stringent as it would expect for its own operations.

v) The Bank or NBFI shall monitor and review the security policies, procedures and controls of the service provider on a regular basis, including periodic expert

reports on security adequacy and compliance in respect of the operations and services provided by the service provider.

vi) The Bank or NBFI shall require the service provider to develop and establish a disaster recovery contingency framework which defines its roles and responsibilities for documenting, maintaining and testing its contingency plans and recovery procedures.

vii) Bank or NBFI shall develop a contingency plan for critical outsourced technology services to protect them from unavailability of services due to unexpected problems of the technology service provider. This may include termination plan and identification of additional or alternate technology service providers for such support and services.

viii) Bank or NBFI shall maintain a service catalogue for all third party services received preserving up-to-date information of each service rendered, service provider name, service type, SLA expiry date, service receiving manager, service reporting, emergency contact person at service provider, last SLA review date, etc.

5.10.3 Service Level Agreement

i) There shall have Service Level Agreements between the Bank or NBFI and vendors.

ii) The Annual Maintenance Contract (AMC) with the vendor shall be active and currently in-force.

iii) Dashboard with significant details for SLAs and AMCs shall be prepared and kept updated.

iv) Bank or NBFI shall ensure that the equipment does not contain sensitive live data when hardware is taken by the service provider for servicing/ repairing.

v) The requirements and conditions covered in the agreements would usually include performance targets, service levels, availability, reliability, scalability, compliance, audit, security, contingency planning, disaster recovery capability and backup processing facility.

vi) Service contracts with all service providers including third-party vendors shall include:

a) Pricing

b) Measurable service/deliverables

c) Timing/schedules

d) Confidentiality clause

e) Contact person names (on daily operations and relationship levels)

f) Roles and responsibilities of contracting parties including an escalation matrix

g) Renewal period

h) Modification clause

i) Frequency of service reporting

j) Termination clause

k) Penalty clause

l) Warranties, including service suppliers' employee liabilities, 3rd party liabilities and the related remedies

m) Geographical locations covered

n) Ownership of hardware and software

o) Documentation (e.g. logs of changes, records of reviewing event logs)

p) Right to have information system audit conducted (internal or external).

6. PCI-DSS, BS7799 and ISO 27000

6.1. PCI-DSS

6.1.1 What is PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS) is an established information security standard which applies to any organization involved in the processing, transmission, and storage of credit card information. Created and overseen by an independent agency, the PCI Security Standards Council (PCI SSC), PCI DSS is designed to improve the security of payment card transactions and to reduce credit card fraud.

The PCI SSC was founded in 2006 as a joint venture between the five largest payment card brands (Visa, MasterCard, American Express, Discover, and JCB). Its goal was to create a clear and interoperable set of standards for protecting consumer information. Although the SSC does not enforce compliance itself, the PCI DSS is now widely accepted and applies to all organizations dealing with credit, debit, or cash card information, regardless of size or industry.

6.1.2. PCI DSS certification

PCI certification ensures the security of card data at your business through a set of requirements established by the PCI SSC. These include a number of commonly known best practices, such as:

- Installation of firewalls
- Encryption of data transmissions
- Use of anti-virus software

In addition, businesses must restrict access to cardholder data and monitor access to network resources.

PCI-compliant security provides a valuable asset that informs customers that your business is safe to transact with. Conversely, the cost of noncompliance, both in monetary and reputational terms, should be enough to convince any business owner to take data security seriously.

A data breach that reveals sensitive customer information is likely to have severe repercussions on an enterprise. A breach may result in fines from payment card issuers, lawsuits, diminished sales and a severely damaged reputation.

After experiencing a breach, a business may have to cease accepting credit card transactions or be forced to pay higher subsequent charges than the initial cost of security compliance. The investment in PCI security procedures goes a long way toward ensuring that other aspects of your commerce are safe from malicious online actors.

6.1.3. PCI DSS Compliance levels

PCI compliance is divided into four levels, based on the annual number of credit or debit card transactions a business processes. The classification level determines what an enterprise needs to do to remain compliant.

- **Level 1**: Applies to merchants processing more than six million real-world credit or debit card transactions annually. Conducted by an authorized PCI auditor, they must undergo an internal audit once a year. In addition, once a quarter they must submit to a PCI scan by an Approved Scanning Vendor (ASV).
- **Level 2**: Applies to merchants processing between one and six million real-world credit or debit card transactions annually. They're required to complete an assessment once a year using a Self-Assessment Questionnaire (SAQ). Additionally, a quarterly PCI scan may be required.
- **Level 3**: Applies to merchants processing between 20,000 and one million e-commerce transactions annually. They must complete a yearly assessment using the relevant SAQ. A quarterly PCI scan may also be required.
- **Level 4**: Applies to merchants processing fewer than 20,000 e-commerce transactions annually, or those that process up to one million real-world transactions. A yearly assessment using the relevant SAQ must be completed and a quarterly PCI scan may be required.

6.1.4. PCI DSS requirements

The PCI SSC has outlined 12 requirements for handling cardholder data and maintaining a secure network. Distributed between six broader goals, all are necessary for an enterprise to become compliant.

Secure network

1. A firewall configuration must be installed and maintained

2. System passwords must be original (not vendor-supplied)

Secure cardholder data
3. Stored cardholder data must be protected
4. Transmissions of cardholder data across public networks must be encrypted

Vulnerability management
5. Anti-virus software must be used and regularly updated
6. Secure systems and applications must be developed and maintained

Access control
7. Cardholder data access must be restricted to a business need-to-know basis
8. Every person with computer access must be assigned a unique ID
9. Physical access to cardholder data must be restricted

Network monitoring and testing
10. Access to cardholder data and network resources must be tracked and monitored
11. Security systems and processes must be regularly tested

Information security
12. A policy dealing with information security must be maintained

6.1.5. Understanding PCI DSS compliance levels

There are four PCI DSS compliance levels that categorize merchants by the volume of transactions they process each year. As larger merchants are responsible for more individual transactions, they also represent bigger targets and potentially expose more people to risk. As a result, the compliance levels for higher transaction volumes correspond to more stringent compliance requirements.

Merchant level	Applicability	Compliance requirements
1	Any merchant processing more than 6 million payment card transactions per year, as well as some merchants specifically designated by members of the SSC	1. Report on compliance 2. Vulnerability scan 3. Attestation of compliance
2	All merchants processing between 1 million and 6 million transactions per year	1. Self-Assessment questionnaire 2. Vulnerability scan 3. Attestation of compliance

Merchant level	Applicability	Compliance requirements
3	Merchants processing between 20,000 and 1 million e-commerce transactions per year	1. Self-Assessment Questionnaire 2. Vulnerability scan 3. Attestation of Compliance
4	Merchants processing less than 20,000 e-commerce transactions or less than 1 million transactions generally per year	1. Self-Assessment Questionnaire 2. Vulnerability scan 3. Attestation of Compliance

Every compliance level involves some permutation of just four specific requirements. The (1) Self-Assessment Questionnaire (SAQ), (2) vulnerability scan, (3) Attestation of Compliance (AOC), and (4) Report on Compliance (ROC) are all procedures used by third-party assessors to assess PCI DSS compliance. These are narrated below:

1. Self-Assessment Questionnaire (SAQ)

The SAQ consists of a variety of yes or no questions that are intended to evaluate whether an entity is complying with PCI DSS. It must be completed by all merchants who do not require a Report on Compliance.

A variety of questionnaires exist, so merchants and service providers must determine which of the specific forms applies to them before completing the SAQ. This selection is primarily based on how the business accepts and processes card payments. For example, merchants who use online payment applications but do not store cardholder data should fill out SAQ-C specifically. Businesses can use the resources on the PCI website to make sure they pick the correct SAQ form.

Depending on the specific questionnaire used, the SAQ can vary in size from about 20 to over 300 questions. Merchants should answer the questions on the SAQ carefully and candidly to correctly determine whether they are complying with PCI DSS.

2. Vulnerability scan

A vulnerability scan is an external scan of a merchant or service provider’s public internet and consumer-facing payment applications and portals. These scans are performed by an Approved Scanning Vendor (ASV) appointed by the PCI SSC to evaluate compliance with PCI DSS at a practical level.

ASVs use a remote tool to detect any vulnerabilities or data security risks in the scanned organization's systems. These scans must be performed on a quarterly basis (once every 90 days).

Almost all merchants must undergo a scan, regardless of applicable compliance level. However, some merchants who complete an SAQ might be exempt, based on the same subclassification used to select the appropriate SAQ form. Specifically, entities qualifying for SAQ A-EP, B-IP, C, and D (merchant or service provider) are all obligated to pass the vulnerability scan requirement while SAQ A, B, C-VT, and PEPE-HW are not.

3. Attestation of Compliance (AOC)

The AOC requirement applies to all merchants seeking to adhere to PCI DSS, regardless of compliance level. This document is signed and submitted by the merchant or service provider if they are completing their own questionnaire, or by an assessor in the case of merchants with the Report on Compliance requirement.

There is one version of the AOC for each type of SAQ form. A merchant completing an SAQ 'A' questionnaire should then use the corresponding AOC 'A' document, for example.

The AOC is simply a declaration of the final results of any PCI DSS assessment. The document ultimately serves as evidence of PCI DSS compliance.

4. Report on Compliance (ROC)

Unlike the SAQ, a ROC is completed by a Qualified Security Assessor (QSA), rather than the merchant. QSAs, like scanning vendors, are third parties approved by the PCI SCC to independently assess PCI DSS compliance.

After completion, the QSA submits the report directly to the assessed merchant's bank. ROCs are required of only the largest, highest-risk merchants and vendors. They are a more stringent equivalent to the self-reporting questionnaires completed at other compliance levels.

Ref: Imperva website and talend website.

6.2. BS7799

6.2.1. What is BS7799?

BS7799 is a British Standard that defines “code of best practices” for an Information Security Management System (ISMS).

BS7799 is an open framework that would be applicable to any enterprise interested in improving security.

The BS 7799 / ISO 17799 standard is written and published in two parts:

1) BS 7799 Part 1: Code of practice for information security management is a guide containing advice and recommendations to ensure the security of a company’s information according to ten fields of application.

2) BS 7799 Part 2: Information security management -- specifications with guidance for use provides recommendations for establishing an effective Information Security Management System (ISMS). At audit time, this document serves as the assessment guide for certification.

6.2.2. History of BS 7799

For over a hundred years, the *British Standards Institution* (BSI) has carried out studies for the purpose of establishing effective, high-quality industry standards. BS 7799 was developed at the beginning of the 1990s in response to industry, government and business requests for the creation of a common information security structure. In 1995, the BS7799 standard was officially adopted.

Four years went by before the publication in May 1999 of a second major version of the BS 7799 standard, incorporating numerous improvements. It was during this period that the International Organization for Standardization (ISO) began to take an interest in the work published by the British institute.

In December 2000, ISO took over the first part of BS 7799, re-baptising it ISO 17799. In September 2002, a revision of the second part of the BS7799 standard was carried out in order to make it consistent with other management standards such as ISO 9001:2000 and ISO 14001:1996 as well as with the principles of the Organization for Economic Cooperation and Development (OECD).

Currently, consultations are taking place at the international level to keep BS 7799 / ISO 17799 at the leading edge of the latest developments.

6.2.3. BS7799 vs ISO 17799

BS7799 Part 1 has been ratified as an ISO standard (ISO/IEC 17799:2000), but Part 2 has not been approved as an ISO standard. Therefore, "ISO 17799" always refers to the international standard based on BS7799 Part 1. ISO 17799 is a code of practice for good security, but does not contain specific requirements for certification. So, an organization can be assessed and certified against BS7799 (part 2), but not for ISO 17799.

6.2.4. Who must comply?

Nobody is required to comply. BS7799 is a voluntary standard of best practices that can be used as a measure of how secure an environment might be. Some organizations use other standards to define their security controls, however BS7799 is gaining more traction due to its international recognition.

6.2.5. BS7799: Part-I: Security Domains, Objectives and Controls

There are 10 areas (domains) of security controls covered by BS7799, 36 security objectives and 127 security controls. A brief overview of each of the10 domains are given below:

6.2.5.1. Domain-1: Security policy

i) Information security policy

A policy document should be published, and all employees should be aware of its existence. This policy should be approved by top management.

6.2.5.2. Domain-2: Security organization

i) Information security infrastructure

A management framework should be established to initiate and control the implementation of information security within the organization.

ii) Security of third party access

Access to the organization's information processing facilities by third parties should be controlled.

The security of organizational information processing facilities might be put at risk by access from third party locations with inadequate security management. Where there is a business need to connect to a third party location, a risk assessment should be carried out to identify any requirements for specific controls. This risk assessment should take into account: the type of access required, the value of the information, the controls employed by the third party and the implications of this access to the security of the organization's information.

The type of access given to the third party is of special importance; for example, the risks of having access across a network connection are very different from risks resulting from physical access. Different types of access are:

a) Physical access, e.g. to offices, computer rooms, filing cabinets;
b) Logical access, e.g. to an organization's databases, information systems.

iii) Outsourcing

The security of information when the responsibility for information processing has been outsourced to another organization should be maintained strictly.

6.2.5.3. Domain-3: Asset classification and control

i) Accountability for assets

All major information assets should be accounted for and have a nominated owner.

Inventories of assets help to ensure that effective protection is maintained. The process of compiling an inventory of assets is an important aspect of risk management. An organization needs to have complete knowledge of all of its assets and the relative value and importance of these assets. Based on this information an organization can then provide levels of protection Examples of assets associated with information systems are:

a) Information assets: databases and data files, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements, archived information;
b) Software assets: application software, system software, development tools and utilities;
c) Physical assets: computer equipment (processors, monitors, laptops, modems), communications equipment (routers, PABXs, fax machines, answering machines), magnetic media (tapes and disks), other technical equipment (power supplies, air-conditioning units), furniture, accommodation;
d) Services: computing and communications services, general utilities (e.g. heating, lighting, power, air-conditioning).

6.2.5.4. Domain-4: Personnel security

i) Security in job definition and resourcing

Security should be addressed at the recruitment stage, included in job descriptions and contracts, and monitored during an individual's employment. Managers should ensure that job descriptions address all relevant security responsibilities.

Users of organizational information processing facilities should sign an appropriate confidentiality (non-disclosure) agreement. Employees should normally sign such an agreement as part of their initial conditions of employment.

Agency staff and third party users not already covered by an existing contract (containing the confidentiality agreement) should be required to sign a confidentiality agreement prior to connection to organizational information processing facilities.

Confidentiality agreements should be reviewed when there are changes to terms of employment or contract, particularly when employees are due to leave the organization, or contracts are due to end.

ii) User training

Users should be trained in security procedures and the correct use of information processing facilities.

6.2.5.5. Domain-5: Physical and environmental security

The requirements for physical security will vary considerably between organizations, depending on the scale of the information services provided and how these are organized, as well as the sensitivity or criticality of the business activities supported.

i) Secure areas

Critical or sensitive business information processes and facilities to support them should be housed in secure areas.

Such facilities should also be physically protected from unauthorized access, damage and interference. They should be sited in secure areas, protected by a defined security perimeter, with appropriate entry controls and security barriers. The degree of protection provided should be commensurate with the risk determined. A clear desk and clear screen policy is recommended to reduce the risk of unauthorized access or damage to papers and media.

ii) Equipment security

Equipment should be protected from power failures or other electrical anomalies.

Power and telecommunication cabling carrying data or supporting information services should be protected from interception or damage.

An organization's data can be compromised through careless disposal of equipment. It should be noted that 'deleted' data could still be easily retrieved from storage media, as deletion does not necessarily erase the information. Even supposedly erased or overwritten data may be

retrieved using specialist equipment. Storage devices containing very highly sensitive data should be physically destroyed or securely overwritten, which is different from the ordinary 'delete' function.

All items of equipment containing storage media, e.g. fixed hard disks, should be checked to ensure that any sensitive data and licensed software are removed or overwritten prior to disposal. Damaged storage devices containing very sensitive data may require a risk assessment to determine if the items should be destroyed, repaired or discarded.

6.2.5.6. Domain-6: Communications and Operations Management

The level of detail and formality of procedures required to manage and operate information processing and communication facilities will vary considerably according to the size of the organization, type of equipment and the nature and sensitivity of the business applications. For example, an organization highly reliant and dependent on the use of information systems and networking technology will require a much higher degree of protection than an organization that makes less use of such technology and is not dependent on it. In principle, the same security processes should be applied, but with appropriate interpretation.

i) Operational procedures and responsibilities

Responsibilities and procedures for the management and operation of all information processing facilities should be established.

Appropriate operating instructions and incident response procedures should be developed to support this. The principle of segregation of duties (see 6.1.3) should be applied, where appropriate, to reduce the risk of negligent or deliberate system misuse.

Procedures should be created and maintained for all operational information processing systems to ensure the correct and secure operation of such systems. Documented procedures should also be prepared for system development, maintenance or testing work, especially if it requires the support or attention of other organizational functions, e.g. computer operations. All operating procedures should be treated as formal documents, changes to which may only be approved by authorized management. The operating procedures should be maintained and reviewed at least annually. One purpose of the operating procedures is to specify the rules necessary to comply with the information security policy for the business application in daily operations. For example, the information security policy might specify that certain equipment should be kept in rooms that are locked during silent hours. The operating procedures should state who will be responsible for locking and opening the rooms, where the key is held and the times the rooms are open.

Segregation of duties

Segregation of duties minimizes the risk of accidental or deliberate system misuse. Consideration should therefore be given to separating the management or execution of certain duties, or of areas of responsibility, in order to reduce opportunities for unauthorized modification or misuse of data or services. In particular, it is recommended that the same employees do not carry out the following functions;

a) Business system use;
b) Data entry;
c) Computer operation;
d) Network management;
e) System administration;
f) Systems development and maintenance;
g) Change management;

ii) Housekeeping

Routine procedures should be established for taking back-up copies of data and rehearsing their timely restoration, logging events and faults and, where appropriate, monitoring the equipment environment.

6.2.5.7. Domain-7: Access control

i) Business requirement for access control

Access to computer information and network services and data should be controlled on the basis of business requirements. This should take account of policies for information dissemination and entitlement.

ii) User access management

Formal procedures should be in place to control the allocation of access rights to information systems and services.

The procedures should cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

iii) User responsibilities

The co-operation of authorized users is essential for effective security.

Users should be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment. Where appropriate, a record of user access should be maintained to aid investigations in case of incidents.

Users should follow good security practices in the selection and use of passwords.

Users should ensure that unattended equipment has appropriate protection. Equipment installed in user areas, e.g. workstations or file servers, may require specific protection from unauthorized access when left unattended for an extended period. All users and contractors should be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection.

iv) Network access control

Connections to networked services should be controlled.

This is necessary in order to ensure that connected users or computer services do not compromise the security of any other networked services. Controls should include the following:

a) Appropriate interfaces between networked services;
b) Appropriate authentication mechanisms for remote users and equipment;
c) Control of user access to information services.

Users should only be provided with direct access to the services that they have been specifically authorized to use. The network and computer services that can be accessed by an individual user or from a particular terminal should be consistent with the business access control policy.

Large networks may need to be divided into separate physical and logical domains. Networks are increasingly being extended beyond traditional organizational boundaries, as business partnerships are formed that may require the interconnection or sharing of information processing and networking facilities. Such extensions might increase the risk of unauthorized access to already existing information systems that use the network, some of which might require protection from other network users because of their sensitivity or criticality. In such circumstances, the introduction of controls within the network, to segregate groups of information services, users and information systems, should be considered.

A wide range of public or private network services is available, some of which offer value-added services. Network services may have unique (possibly complex) security characteristics. Organizations using network services should ensure that their network provider gives a clear description of the security attributes of all services used, and should establish the security implications for the confidentiality, integrity and availability of business applications.

v) Computer access control

Access to computer facilities should be controlled. Such access should be restricted to authorized users.

All users should have a unique identifier (user ID) for their personal and sole use, to ensure that activities can subsequently be traced to the responsible individual. User IDs should not give any indication of the user's privilege level, e.g. manager, supervisor.

vi) Application access control

Logical access controls should be used to control access to application systems and data.

Logical access to software and data should be restricted to authorized users. Application systems should:

a) Control user access to data and application system functions, in accordance with a defined business access control policy;
b) Provide protection from unauthorized access for any utility and operating system software that is capable of overriding system or application controls;
c) Not compromise the security of other systems with which information resources are shared;
d) Be able to provide access to information to the owner only, other nominated authorized individuals, or defined groups of users.

vii) Monitoring system access and use

Systems should be monitored to ensure conformity to access policy and standards.

Audit logs recording exceptions and other security-relevant events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.

6.2.5.8. Domain-8: Systems development and maintenance

i) Security requirements of systems

This will include infrastructure, business applications and user-developed applications. Note also that in some cases, the design and implementation of the business process supporting the application or service is crucial for security. Security requirements should be identified and agreed prior to the development of information systems.

ii) Security in application systems

Appropriate controls and audit trails should be designed into application systems, including user written applications.

Data encryption should be considered for the protection of highly sensitive and/or valuable data. Encryption is the process of transforming data into an unintelligible form, to safeguard its confidentiality during transmission or in storage. The process of encryption uses one of two types of cryptographic technique as described below.. The level of protection provided by encryption depends on the strength of the underlying cryptographic algorithm, size of key space, length of key and the secure management of the keys.

6.2.5.9. Domain-9: Business continuity management

i) Aspects of business continuity management

Business continuity management reduces the damage caused by disasters and security failures (which may be caused by, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventative and recovery measures.

The consequences of disasters, security failures and loss of service should be analysed. Contingency plans should be developed and implemented to ensure that critical processes could be restored within the required time scales. Such plans should be maintained and practised to become an integrated component of all other management processes and be accepted as such by staff members, suppliers and contractors.

Business continuity planning should include measures to identify and reduce risks, limit the consequences if a damaging incident occurs, and ensure the timely resumption of essential operations.

There should be a managed process in place for developing and maintaining business continuity throughout the organization. The process should bring together the following key elements of business continuity management:

a) An understanding of the risks faced by the business, in terms of their likelihood and their impact, including an identification and prioritisation of critical business processes;

b) An understanding of the impact interruptions of varying magnitudes and lengths will have to the business (it is important that solutions are found that will handle smaller incidents, as well as serious incidents threatening the ongoing viability of the organization), and the establishment of business objectives and priorities for each information system;

c) The formulation and documentation of a business continuity strategy commensurate with the agreed business objectives and priorities;

d) The formulation and documentation of business continuity plans in line with the agreed strategy;

e) The recognition that the plans and processes put in place need regular testing and updating as the business being protected evolves;

f) The insurance that the management of business continuity, and the processes to achieve it, are embedded into the organization's processes and structure. Responsibility for co-ordinating the process and status reporting should be assigned at an appropriate level within the organization, e.g. at the information security forum.

6.2.5.10. Domain-10: Compliance

i) Compliance with legal requirements

The design, operation, use and management of information systems may be subject to statutory, regulatory and contractual security requirements.

All relevant statutory, regulatory and contractual requirements should be explicitly defined and documented for each information system. The specific controls and individual responsibilities to meet these requirements should be similarly defined and documented.

Advice on specific legal requirements should be sought from the organization's legal advisers, or suitably qualified legal practitioners. Legislative requirements vary from country to country and for information created in one country that is transmitted to another country (i.e. trans-border data flow).

ii) System audit considerations

Audit requirements and activities involving checks on operational systems should be carefully planned and agreed, to minimize the risk of disruptions to business processes. The following should be observed:

a) Audit requirements should be agreed with appropriate management;
b) The scope of the checks should be agreed and controlled;
c) The checks should be limited to read-only access to software and data;
d) Other types of access (other than read-only) should only be allowed for isolated copies of system files, which should be erased when the audit is completed;
e) IT resources for performing the checks should be explicitly identified and made available;
f) Requirements for special or additional processing should be identified and agreed;
g) All access should be monitored and logged to produce a reference trail;
h) All procedures, requirements and responsibilities should be documented.

6.2.6. BS 7799: Part-II: ISMS and Certification

5.2.6.1. Compliance/Certification Process

Compliance with BS 7799 is a formal and sometimes complex process. The steps defined by the British Standards Institute (BSI) are as follows:

a) Establish a management framework as defined by the standard
b) BSI will provide an estimate of costs and timeframes for formal assessment
c) Submit a formal application to BSI
d) BSI will undertake a review of the enterprise's stated security and risk policies. This will help identify any weaknesses in the management system that need to be resolved
e) BSI will conduct an on-site assessment
f) On successful completion of the audit, a certificate of registration will be issued that identifies the scope of the ISMS.

5.2.6.2. What is an ISMS?

"To establish the organization's information security policy and objectives... and then meet these objectives."

An Information Security Management System (ISMS) provides a systematic approach to managing sensitive information in order to protect it. It encompasses employees, processes and information systems.

6.3. ISO 27001

ISO 27001 is the international standard that provides the specification for an information security management system (ISMS). ISO 27001 is technology and vendor neutral and is applicable to all organisations – irrespective of their size, type or nature. The Standard is designed to help organisations manage their information security processes in line with international best practice while optimizing costs.

6.3.1. Benefits of implementing an ISMS

1. Secures your information in all its forms
2. Increases resilience to cyber attacks
3. Provides a centrally managed framework
4. Offers organisation-wide protection
5. Helps respond to evolving security threats
6. Reduces costs associated with information security
7. Protects confidentiality, availability and integrity of data

8. Improves company culture

6.3.2. What are the 14 domains of ISO 27001?

There are 14 “domains” A of ISO 27001 are:

1. Information security policies: The controls in this section describe how to handle information security policies.

2. Organization of information security: The controls in this section provide the basic framework for the implementation and operation of information security by defining its internal organization (e.g., roles, responsibilities, etc.), and through the organizational aspects of information security, like project management, use of mobile devices, and teleworking.

3. Human resource security: The controls in this section ensure that people who are under the organization’s control are hired, trained, and managed in a secure way; also, the principles of disciplinary action and terminating the agreements are addressed.

4. Asset management: The controls in this section ensure that information security assets (e.g., information, processing devices, storage devices, etc.) are identified, that responsibilities for their security are designated, and that people know how to handle them according to predefined classification levels.

5. Access control: The controls in this section limit access to information and information assets according to real business needs. The controls are for both physical and logical access.

6. Cryptography: The controls in this section provide the basis for proper use of encryption solutions to protect the confidentiality, authenticity, and/or integrity of information.

7. Physical and environmental security: The controls in this section prevent unauthorized access to physical areas, and protect equipment and facilities from being compromised by human or natural intervention.

8. Operations security: The controls in this section ensure that the IT systems, including operating systems and software, are secure and protected against data loss. Additionally, controls in this section require the means to record events and generate evidence, periodic verification of vulnerabilities, and make precautions to prevent audit activities from affecting operations.

9. Communications security: The controls in this section protect the network infrastructure and services, as well as the information that travels through them.

10. System acquisition, development and maintenance: The controls in this section ensure that information security is taken into account when purchasing new information systems or upgrading the existing ones.

11. Supplier relationships: The controls in this section ensure that outsourced activities performed by suppliers and partners also use appropriate information security controls, and they describe how to monitor third-party security performance.

12. Information security incident management: The controls in this section provide a framework to ensure the proper communication and handling of security events and incidents, so that they can be resolved in a timely manner; they also define how to preserve evidence, as well as how to learn from incidents to prevent their recurrence.

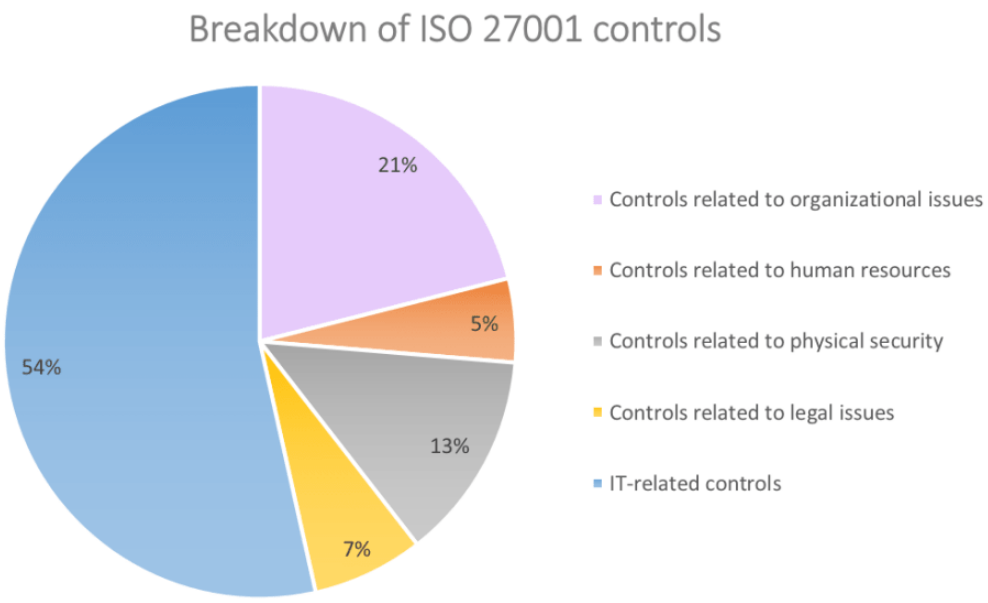
13. Information security aspects of business continuity management: The controls in this section ensure the continuity of information security management during disruptions, and the availability of information systems.

14. Compliance: The controls in this section provide a framework to prevent legal, statutory, regulatory, and contractual breaches, and audit whether information security is implemented and is effective according to the defined policies, procedures, and requirements of the ISO 27001 standard.

A closer look at these domains shows us that managing information security is not only about IT security (i.e., firewalls, anti-virus, etc.), but also about managing processes, legal protection, managing human resources, physical protection, etc.

6.3.3. How many controls are there in ISO 27001?

ISO 27001 has 114 controls organized in the 14 sections listed above.



6.3.4. What is "ISO 27001 certified"?

A company can go for ISO 27001 certification by inviting an accredited certification body to perform the certification audit and, if the audit is successful, to issue the ISO 27001 certificate to the company. This certificate will mean that the company is fully compliant with the ISO 27001 standard.

An individual can go for ISO 27001 certification by going through ISO 27001 training and passing the exam. This certificate will mean that this person has acquired the appropriate skills during the course.

Ref: 27000.org

7. Legal Framework in Bangladesh

7.1. Cyber Law

7.1.1. What is Cyber Law?

In Simple way we can say that cyber crime is unlawful acts wherein the computer is either a tool or a target or both

Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Bangladesh Penal Code. The

abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information and Communication Technology Act, 2006 (ICT Act-2006).

7.1.2. Cyber Crime Categories:

We can categorize Cyber crimes in two ways:

a) The Computer as a Target: using a computer to attack other computers e.g. Hacking, Virus/Worm attacks, DOS attack etc.

b) The computer as a weapon: using a computer to commit real world crimes e.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc.

Cyber Crime regulated by Cyber Laws or Internet Laws.

7.1.3. Cyber Crimes Activities:

Technological advancements have created new possibilities for criminal activity, in particular the criminal misuse of information technologies for conducting cyber crimes such as:

i) Unauthorized access & Hacking:

Access means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network.

Unauthorized access would therefore mean any kind of access without the permission of either the rightful owner or the person in charge of a computer, computer system or computer network.

Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money.

By hacking web server taking control on another persons website called as web hijacking

ii) Trojan Attack:

The program that acts like something useful but do the things that are quiet damping. The programs of this kind are called as Trojans. The name Trojan Horse is a popular.

Trojans come in two parts, a Client part and a Server part. When the victim (unknowingly) runs the server on its machine, the attacker will then use the Client to connect to the Server and start using the trojan.

TCP/IP protocol is the usual protocol type used for communications, but some functions of the trojans use the UDP protocol as well.

iii) Virus and Worm attack:

A program that has capability to infect other programs and make copies of itself and spread into other programs is called virus.

Programs that multiply like viruses but spread from computer to computer are called as worms.

iv) E-mail related crimes:

a. Email spoofing

Email spoofing refers to email that appears to have been originated from one source when it was actually sent from another source.

b. Email Spamming

Email "spamming" refers to sending email to thousands and thousands of users - similar to a chain letter.

c. Sending malicious codes through email

E-mails are used to send viruses, Trojans etc through emails as an attachment or by sending a link of website which on visiting downloads malicious code.

d. Email bombing

E-mail "bombing" is characterized by abusers repeatedly sending an identical email message to a particular address.

e. Sending threatening emails

f. Defamatory emails

g. Email frauds

v) Denial of Service (DoS) attacks:

Flooding a computer resource with more requests than it can handle. This causes the resource to crash thereby denying access of service to authorized users.

vi) Pornography:

This would include pornographic websites; pornographic material produced using computers and use of internet to download and transmit pornographic videos, pictures, photos, writings etc.

Adult entertainment is largest industry on internet. There are more than 420 million individual pornographic webpages today.

vii) Forgery:

Counterfeit currency notes, postage and revenue stamps, mark sheets etc can be forged using sophisticated computers, printers and scanners.

Also impersonate another person is considered forgery.

viii) IPR Violations:

These include software piracy, copyright infringement, trademarks violations, theft of computer source code, patent violations etc.

Domain names are also trademarks and protected by ICANN's domain dispute resolution policy and also under trademark laws.

Cyber Squatters registers domain name identical to popular service provider's domain so as to attract their users and get benefit from it.

ix) Cyber Terrorism:

Targeted attacks on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks are the most likely targets. Others like police, medical, fire and rescue systems etc.

Cyber terrorism is an attractive option for modern terrorists for several reasons.

1. It is cheaper than traditional terrorist methods.
2. Cyber terrorism is more anonymous than traditional terrorist methods.
3. The variety and number of targets are enormous.
4. Cyber terrorism can be conducted remotely, a feature that is especially appealing to terrorists.
5. Cyber terrorism has the potential to affect directly a larger number of people.

x) Banking/Credit card Related crimes:-

In the corporate world, Internet hackers are continually looking for opportunities to compromise a company's security in order to gain access to confidential banking and financial information.

Use of stolen card information or fake credit/debit cards is common.

Bank employee can grab money using programs to deduct small amount of money from all customer accounts and adding it to own account also called as salami.

xi) E-commerce/ Investment Frauds:

Sales and Investment frauds is an offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities.

Merchandise or services that were purchased or contracted by individuals online are never delivered.

The fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site.

Investors are enticed to invest in this fraudulent scheme by the promises of abnormally high profits.

xii) Sale of illegal articles:

This would include trade of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication.

xiii) Online gambling:

There are millions of websites hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering.

xiv) Defamation:

Defamation can be understood as the intentional infringement of another person's right to his good name.

Cyber Defamation occurs when defamation takes place with the help of computers and / or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends. Information posted to a bulletin board can be accessed by anyone. Cyber defamation is also called as Cyber smearing.

xv) Identity Theft:

Identity theft is the fastest growing crime in countries like America.

Identity theft occurs when someone appropriates another's personal information without their knowledge to commit theft or fraud.

Identity theft is a vehicle for perpetrating other types of fraud schemes.

xvi) Data diddling:

Data diddling involves changing data prior or during input into a computer.

In other words, information is changed from the way it should be entered by a person typing in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file.

It also includes automatic changing the financial information for some time before processing and then restoring original information.

xvii) Theft of Internet Hours:

Unauthorized use of Internet hours paid for by another person.

By gaining access to an organization’s telephone switchboard (PBX) individuals or criminal organizations can obtain access to dial-in/dial-out circuits and then make their own calls or sell call time to third parties.

Additional forms of service theft include capturing 'calling card' details and on-selling calls charged to the calling card account, and counterfeiting or illicit reprogramming of stored value telephone cards.

xviii) Theft of computer system (Hardware):

This type of offence involves the theft of a computer, some part(s) of a computer or a peripheral attached to the computer.

xix) Physically damaging a computer system:

Physically damaging a computer or its peripherals either by shock, fire or excess electric supply etc.

xx) Breach of Privacy and Confidentiality

Privacy

Privacy refers to the right of an individual/s to determine when, how and to what extent his or her personal data will be shared with others.

Breach of privacy means unauthorized use or distribution or disclosure of personal information like medical records, sexual preferences, financial status etc.

Confidentiality

It means non disclosure of information to unauthorized or unwanted persons.

In addition to Personal information some other type of information which useful for business and leakage of such information to other persons may cause damage to business or person, such information should be protected.

Generally for protecting secrecy of such information, parties while sharing information forms an agreement about he procedure of handling of information and to not to disclose such information to third parties or use it in such a way that it will be disclosed to third parties.

Many times party or their employees leak such valuable information for monitory gains and causes breach of contract of confidentiality.

Special techniques such as Social Engineering are commonly used to obtain confidential information.

7.2. ICT Act

7.2.1. Introduction

After the invention of computers and improvement in digital technology and communication systems dramatic changes have taken place in our lives. Business transactions are being made with the help of computers. However in our country the people were reluctant to conduct business or conclude transactions in electronic form due to lack of legal framework. Many legal provisions recognize paper based records and documents bearing signature of parties and make them admissible in evidence in various disputes. Transactions in electronic form were often not recognized in courts. Many legal rules assume the existence of paper records and documents, signed records, original records, physical cheques, face to face meetings, etc. As more and more

activities are carried out by electronic means, it becomes more and more important that evidence of these activities be available to demonstrate legal rights and obligations that flow from them.

7.2.2. Applicable fields of ICT Act-2006

In view of the above, an act was enacted in the name of 'Information and Communication Technology Act-2006' in 2006 which shall apply to-

- a Negotiable Instrument
- the creation, performance or enforcement of a power of attorney
- a Trust
- a Will
- any Contract for the Sale or Conveyance of Immovable property or any interest in such property
- documents of title
- any such class of documents or transactions as may be notified by the Government in the Official Gazette.

7.2.3. Objectives

The main objectives of the Information and Communication Technology Act-2006 are to:

1. Eliminates barriers to e-commerce,
2. Promotes legal and business infrastructures to secure e-transactions,
3. Facilitates electronic filing in government agencies,
4. Ensures efficient delivery of electronic records from government offices,
5. Help maintain the latest technology by freeing it from nuisance as punitive provisions publishing obscene or defamatory information in electronic form,
6. Ensures ten years imprisonment and a fine of up to Taka 10 million (Tk.1.00 Crore) or both, for the cyber offenders
7. Powers of Police Officers and Other Officers,
8. Establishment of Cyber Appellate Tribunal.

7.2.4. Selected clauses

Some of the clauses of the Act are presented below in a simplified form:

Clause-5. Authentication of Electronic Records by Digital Signature

(1) Subject to the provisions of sub-clause (2) any subscriber may authenticate an electronic record by affixing his digital signature.

(2) The authentication of the electronic record shall be effected by the use of an open technique or an established equipment or technique developed for crating electronic signature.

Clause-6. Legal Recognition of Electronic Records

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is

(a) rendered or made available in an electronic form; and
(b) accessible so as to be usable for a subsequent reference

Clause-7. Legal recognition of Electronic Signature

Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document should be signed or bear the signature of any person then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Government.

Clause-8. Use of Electronic Records and Digital Signatures in Government and its agencies

Where any law requires –

(a) the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;

(b) the issue or grant of any licence, permit, sanction or approval by whatever name called in a particular manner;

(c) the receipt or payment of money in a particular manner,

then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the Government.

Clause-13. Attribution, Acknowledgment and Dispatch of Electronic Records

An electronic record shall be attributed to the originator

(a) if it was sent by the originator himself;

(b) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or

(c) by an information system programmed by or on behalf of the originator to operate automatically.

Chapter-5: CONTROLLER & CERTIFYING AUTHORITIES

Clause-18. Appointment of Controller and other officers

(1) The Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification appoint such number of Deputy Controllers and Assistant Controllers as it deems fit.

Clause-19. The Controller may perform all or any of the following functions, namely –

(a) exercising supervision over the activities of the Certifying Authorities;

(b) certifying public keys of the Certifying Authorities

(c) laying down the standards to be maintained by the Certifying Authorities;

(d) specifying the qualifications and experience which employees of the Certifying Authorities should possess;

(e) specifying the conditions subject to which the Certifying Authorities shall conduct their business;

(f) specifying the content of written, printed or visual material and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the Public Key;

(g) specifying the form and content of a Digital Signature Certificate and the key;

(h) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;

(i) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;

(j) facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;

(k) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;

(l) resolving any conflict of interests between the Certifying Authorities and the subscribers;

(m) laying down the duties of the Certifying Authorities;

(n) maintaining a data-base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

Clause-20. Recognition of foreign Certifying Authorities

(1) Subject to such conditions and restrictions as may be specified by regulations, the Controller may with the previous approval of the Central Government, and by notification in the Official Gazette, recognise any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.

(2) Where any Certifying Authority is recognised under sub-section (1), the Digital Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.

Clause-22. License to issue digital signature certificates

(1) Any person may make an application, to the Controller, for a licence to issue Digital Signature Certificates.

(3) No licence shall be issued unless the applicant fulfills such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities, which are necessary to issue Digital Signature Certificates as may be prescribed by the Central Government.

(4) A license granted under this section shall –

(a) be valid for such period as may be prescribed by the Central Government;

(b) not be transferable or heritable;

(c) be subject to such terms and conditions as may be specified by the regulations.

Clause-31. Certifying Authority to follow certain procedures

Every Certifying Authority shall-

(a) make use of hardware, software, and procedures that are secure from intrusion and misuse:

(b) provide a reasonable level of reliability in its services which arc reasonably suited to the performance of intended functions;

(c) adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured; and

(d) observe such other standards as may be specified by regulations.

Clause-36. Certifying Authority to issue Digital Signature Certificate

(1) Any person may make an application to the Certifying Authority for the issue of a Digital Signature Certificate in such form as may be prescribed by the Government.

(2) Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.

(3) On receipt of an application under sub-section (1), the Certifying Authority may, after consideration of the certification practice statement or the other statement under sub-section

(4) and after making such enquiries as it may deem fit, grant the Digital Signature Certificate or for reasons to be recorded in writing, reject the application

Provided that no Digital Signature Certificate shall be granted unless the Certifying Authority is satisfied that -

(a) the applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate;

(b) the applicant holds a private key, which is capable of creating a digital signature;

(c) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant.

Chapter-6: DUTIES OF SUBSCRIBERS

Clause-42. Acceptance of Digital Signature Certificate.

A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of a Digital Signature Certificate - (a) to one or more persons; (b) in a

repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

Chapter-8: PENALTIES AND ADJUDICATION

Clause-54. Penalty for damage to computer, computer system, etc

If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network -

(a) accesses or secures access to such computer, computer system or computer network.

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programs residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder,

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network,

he shall be punished with imprisonment up to ten years, or with fine not more than Taka 10 lac, or with both.

Clause-55. Tampering with Computer Source Documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is

required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine not exceeding Taka three lac, or with both.

Clause-56. Hacking with Computer System

(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person, destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

(2) Whoever commits hacking shall be punished with imprisonment up to ten years, or with fine not exceeding Taka one crore, or with both.

Chapter-8: Part-2: THE CYBER REGULATIONS APPELLATE TRIBUNAL

Clause-68. Establishment of Cyber Appellate Tribunal

(1) The Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Regulations Appellate Tribunal.

(2) The Central Government shall also specify, in the notification referred to in sub-section (1), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.

Review Questions

1. Multiple Choice Questions (MCQ)

i) Near Data Center (NDC) is built in -------- for quick start of operation in case of major or minor breakdown in Data Center (DC).
a) Same City b) Different City c) Same Seismic Zone d) Different Seismic Zone

ii) Which of the following is a major IT shutdown?
a) Database Corrupted b) Server non-functioning c) UPS is not working d) Cooling system is out of order

iii) Which of the following is a remedy for Application Server non-functioning?
a) Active-active clustering b) Network Load Balancing c) Redundant UPS d) Active-Standby System

iv) To prevent unauthorized use of cards in an e-commerce site, Card issuing bank deliver a ----- token to the cardholder for use during e-commerce transaction.
a) OTP b) 2FA c) POS d) ATM

v) Ransomware is a type of malicious software that block access to users in to their IT system unless a -------- is paid.
a) Dollar b) Bitcoin c) Ransom d) Taka

vi) A ------- is first sent to many employees of a bank as attachment of a email narrating attractive offeres.
a) Hacker b) Database c) Router d) Malware

vii) Phishing is presenting a -------.
a) fake email b) fake website c) fake credit card d) fake password

viii) Which of the following is not a crypto currency?
a) Bitcoin b) Ether c) Router d) Petro

2. Fill in the gap(s)

i) For the first time, IT professionals started protecting their database and network placing ------ on the network.

ii) To keep the data safe and available in case of any disaster, IT professionals built ----- and ------ .

iii) Unsatisfied -------- may steal data and handover to the hackers.

iv) Duplicating a credit card by fraudster is called --------.

v) A ------ card can prevent skimming of cards in ATM.

vi) Corrupted ------- are engaged in POS skimming.

vii) DDoS attack is done by attackers to ------ a website.

viii) ------ system and ------ system maintain balance in USD and are most vulnerable to hacking.

Probable Questions

1. What is the difference between ICT Security and Cyber Security?

2. Why Data Centers are very important part of ICT risks?

3. Narrate Business Continuity Threats, Classify Business Discontinuity.

4. Describe different types of Internal Threats.

5. List different threats related to MFS and their remedies.

6. Describe ATM Skimming and POS Skimming? Where you can use the anti-skimming device?

7. What is ATM Jackpotting?

8. How fraud occurs in e-commerce?

9. Describe following cyber treats: DDos, Ransomeware and Malware.

10. What is hacking? How money is unauthorizedly transferred from the client's account by the Hackers?

11. Why Swift and Credit Card is in the risk of cyber treat in Bangladesh?

12. Do you think that Crypto-currency is threat? Why?

13. Put your suggestions to minimize ICT risk and Cyber Treats.

14. Differentiate between Security Standards and Regulations.

15. Name three popular Regulations.

16. Why Banks should acquire "Certification" on popular "Security Standards"?

17. Write ten important points covered in the guideline on "ICT Security for scheduled Banks and Financial Institutes" published by the Bangladesh Bank.

18. With respect to the "ICT Security of scheduled banks and financial institutes" published by the Bangladesh Bank, reply to the following:

    a) Narrate the roles and responsibilities of Board of Directors.

b) Narrate the roles and responsibilities of of ICT Steering Committee.

c) Narrate the roles and responsibilities of ICT Security Committee.

d) What is ICT Risk Governance?

e) What do you know about Change Management?

f) What is Incident Management?

g) What is BYOD?

h) What do you mean by Physical Security of Data Center?

i) Why email management is important?

j) What is User Access Management?

k) What is Business Continuity Plan?

l) What is Disaster Recover Plan?

m) What points to be considered during In-house Software Development?

n) What security mechanism should be undertaken by banks to secure its Internet Banking System?

0) What security mechanism should be undertaken by banks to secure its Credit Cards?

19. What is PCI-DSS? Why Banks should undertake PCI-DSS certification?

20. What is BS 7799? Write history of BS 7799.

21. What is ISO 27001? Write Why banks should acquire certification on ISO 27001 standard?

22. What are the 14 domains of ISO 27001?

23.What is a Cyber Law? Narrate any five of the Cyber Crime activities.

24. Describe ICT Act and mention applicable fields of ICT Act-2006.

25. Write Clause-56: Hacking with Computer System.

Module-E

Document Handling Systems
Additional Banking Applications
& Other Aspects

1. Cheque Processing Systems

Cheque Processing System or Payment system in short, is a means by which funds are transferred among financial institutions, businesses, and persons. Payment systems are considered as the most important factor for the well functioning of a country's financial system and for successful application of monetary policies by the central banks. Moreover, cross-border connections of the payment systems become essential for development of a country and for attracting foreign capital and foreign investors.

1.1. Clearing and Settlement Systems

At present, four clearing systems are operating in Bangladesh. They are:

(a) Bangladesh Bank's Clearing Houses in Dhaka and its branches in seven other cities;

(b) Sonali Bank's Clearing Houses in 31 cities where there are no BB branches;

(c) the BB large value cheque settlement system; and

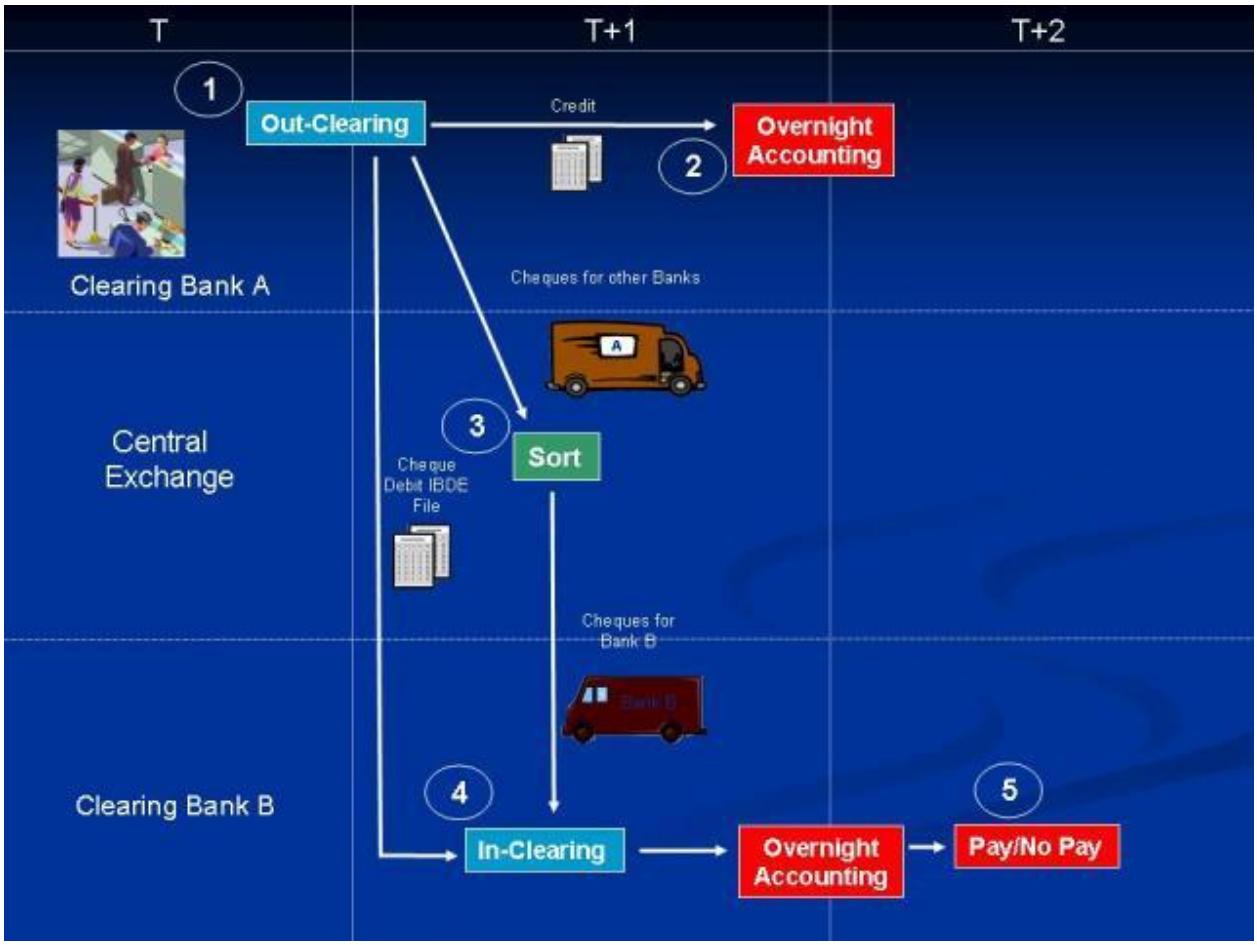
(d) the Bangladesh Bank Foreign Currency Clearing System in Dhaka which clears and settles foreign currency cheques and pay orders by the Forex Reserve and Treasury Management Department (FRTMD).

There are four clearings each day at the BB's clearing house. The first clearing starts at 10:30 am and returns of the first clearing are at 5:30 pm The Same Day clearing starts at 11:00 am and returns occur at 2:00 pm. The instruments cleared through the clearing houses are cheques, bank drafts, pay orders, dividend warrant, etc. drawn on commercial banks and BB. Except Barisal and Rangpur office, other branch offices of BB have a computerized settlement process where the commercial banks, in addition to the physical instruments, present diskettes that contain each bank's paying obligations and receivables from other banks. Compared to the volume in Dhaka and Chittagong, the cheques cleared in outstation branches are insignificant.

1.2. Conventional Cheque Clearing Process

The conventional Cheque clearing process is a fairly time consuming procedure and it involves many manual processes and physical movement of the instruments. It not only increases the time of clearing, also exposed to higher level of risks and frauds as the instruments are moving in various points and through various persons.

The typical cycle of such clearing process is as under:

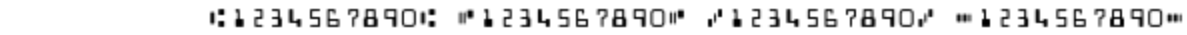


1.3. MICR (Magnetic Ink Character Recognition)

Since the manual or conventional cheque clearing process is time consuming, the introduction of MICR has come into place. Magnetic Ink Character Recognition, or MICR, is a character recognition technology used primarily by the banking industry to facilitate the processing of cheques. The technology allows computers to read information (such as account numbers, cheque numbers and special characters) printed on the bottom of cheques or other financial transaction documents. Unlike barcodes or similar technologies, however, MICR codes can be easily read by humans.

MICR characters are printed in special typefaces with a magnetic ink or toner, usually containing iron oxide. As a machine decodes the MICR text, it first magnetizes the characters in the plane of the paper. Then the characters are passed over a MICR read head, a device similar to the playback head of a tape recorder. As each character passes over the head produces a unique waveform that can be easily identified by the system. MICR technology is used in the banking industry in many countries including Bangladesh because it allows for fast and reliable document processing.

The major MICR fonts used around the world are E-13B and CMC-7. The E-13B character set is as under:



Whereas CMC-7 character set is as follows:

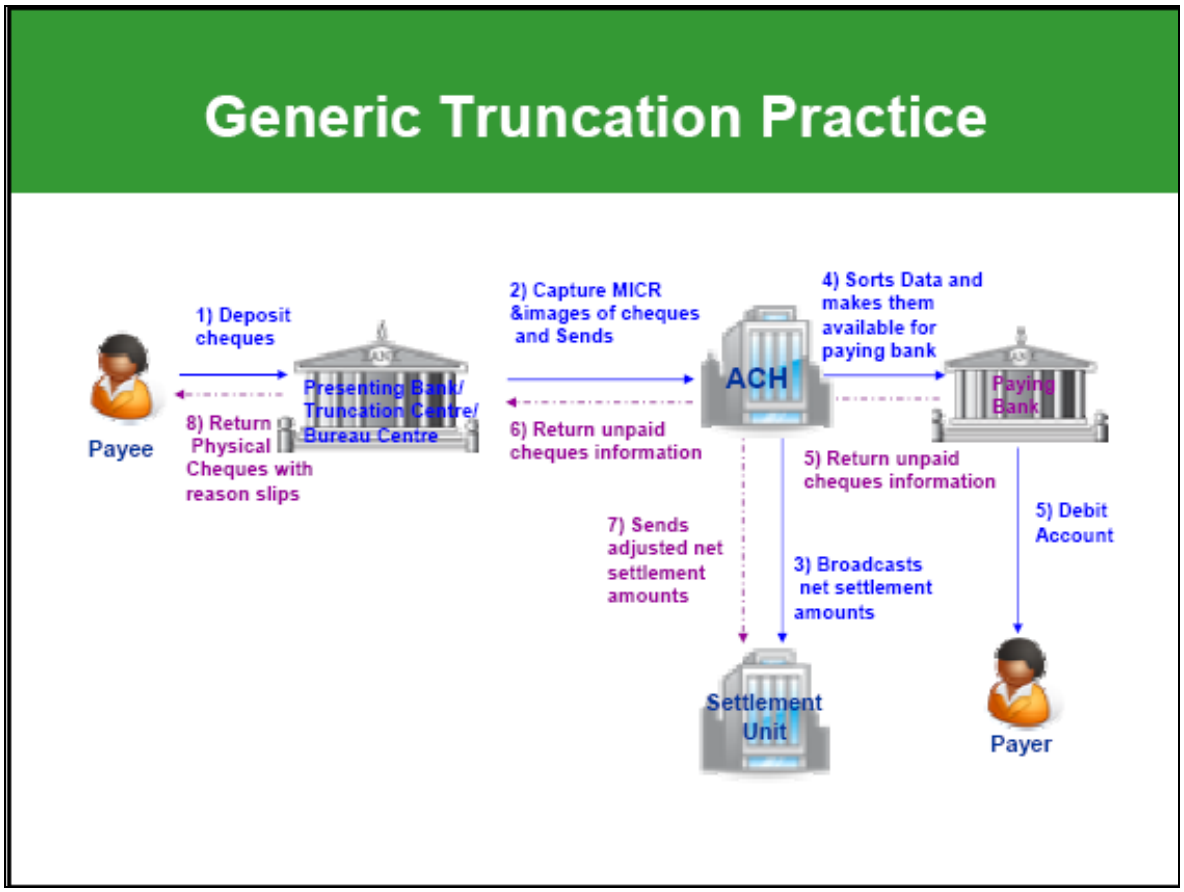
1.4. Cheque Truncation

Cheque Truncation is the process of stopping the flow of the physical cheque issued by a drawer to the drawee branch. The physical instrument will be truncated at some point en-route to the drawee branch and an electronic image of the cheque would be sent to the drawee branch along with the relevant information like the MICR fields, date of presentation, presenting banks etc. Thus with the implementation of cheque truncation, the need to move the physical instruments across branches/ banks would not be required, except in exceptional circumstances. This would effectively reduce the time required for payment of cheques, the associated cost of transit and delay in processing, etc., thus speeding up the process of collection or realization of the cheques.

The Cheque Truncation System, CTS envisages a safe, secured, faster and effective system for clearing of the cheques. In the CTS the presenting bank will capture the data & images of the cheques using their Image Capture System which is internal to them. They have to meet the specifications and standards prescribed for data and images. To ensure security, safety and non-repudiation the PKI (Public Key Infrastructure) is being implemented across the system. The banks will send the captured images and data to the central clearing house for onward transmission to the payee/ drawee banks.

For the above purpose, Bangladesh Bank has provided all the banks a software called Participating Bank Module, PBM which enables them to connect and transmit data in a secure way and with non-repudiation to the Clearing House (CH). The Clearing House will process the data and arrive at the settlement figure for the banks and send the required data to payee/ drawee banks for processing at their end. The drawee/ payee banks will use their PBM mentioned earlier for receiving the data and images from the Clearing House. It will be the responsibility of the drawee bank Capture System to process the inward data and images and generate the return file for unpaid instruments.

The Generic Truncation practices are as under:



The infrastructure required for CTS from bank's end are connectivity from the bank gateway to the clearing house, hardware and software for the CTS applications. Bangladesh Bank shall be providing member banks with the PM and the banks have to procure other hardware and system software for the CH and the application software for their capture systems on their own.

Some of the benefits of such system are:

- Faster clearing cycle
- Better reconciliation/ verification process
- Better Customer Service, Enhanced Customer Window
- T+0 or T+1 day Clearing
- Elimination of Float. Incentive to shift to Credit Push payments
- The jurisdiction of Clearing House can be extended to the entire country. No Geographical Dependence
- Operational Efficiency will benefit the bottom lines of banks
- Minimises Transaction Costs
- Reduces operational risk by securing the transmission route

1.5. RTGS (Real Time Gross Settlement)

Real Time Gross Settlement (RTGS) systems are funds transfer systems where transfer of money or securities takes place from one bank to another on a "real time" and on "gross" basis. This is the fastest possible money transfer system through the banking channel. Settlement in "real time" means payment transaction is not subjected to any waiting period. The transactions are settled as soon as they are processed. "Gross settlement" means the transaction is settled on one to one basis without bunching or netting with any other transaction. Considering that money transfer takes place in the books of the Central Bank, the payment is taken as final and irrevocable.

1.6. BACH (Bangladesh Automated Clearing House)

Bangladesh Bank has taken up the project of automating the payment systems of the country in the name of “Bangladesh Automated Clearing House” (BACH). The project BACH is divided into two parts:

i) BACPS (Bangladesh Automated Cheque Processing Systems) and
ii) BEFTN (Bangladesh Electronic Funds Transfer Network)

1.6.1. Bangladesh Automated Cheque Processing Systems (BACPS)

Bangladesh Bank has launched the BACPS in 2010. BACPS has been implemented with cheque imaging and truncation activities.

Accordingly the cheque design for the Banks has been standardized. The size, security features and paper specifications have been informed to the financial institutions. The new cheque leaf contains Magnetic Ink Character Recognition (MICR) line which has been designed to provide information on the amount, transaction code, clients account information, routing number and the cheque leaf's serial number.

The new routing numbers have been assigned to the bank branches for easy identification of origin and destination of a cheque. The routing number comprises of 9 digits. The first 3 digits are Bank codes, next 2 digits are district codes, following 3 digits are branch code and the last digit is the check digit.

The system will support both intra-regional and inter-regional clearings. The system is based on a centralized processing centre located in Dhaka and its Service Branches at 64 districts. The proposed processes and systems will conform to best practices and also will represent the most cost effective solution for cheque processing. The first phase of BACPS project, i.e, Dhaka Clearing House is in operation since October 7, 2010.

1.6.2. Bangladesh Electronic Funds Transfer Network (BEFTN)

BEFTN will operate as a processing and delivery centre providing for the distribution and settlement of electronic debit and credit instruments among all participating banks. The BEFTN Network is envisaged as a system of participating banks connected with the EFT Operator via communication lines. This network will facilitate the transmission of payments between the banks electronically, which will make faster and efficient means of inter-bank clearing than the existing paper-based system.

The Network will start with simple credit transactions and gradually progress to debit transactions. This will dramatically bring down the operational cost, reduce risk and will also increase the efficiency of the payments process.

BEFTN, a mode of electronic fund transfer, operates on a deferred net settlement (DNS) basis which settles transactions in batches. In DNS, the settlement takes place at a particular point of time. All transactions are held up till that time. For example, if EFT settlement takes place 2 times a day during the week days (as for example at 11.00 am & 3:00 pm), any transaction initiated after a designated settlement time would have to wait till the next designated settlement time. Contrary to this, in RTGS, transactions are processed continuously throughout the RTGS business hours.

2. Additional Banking Applications

2.1. ERP Software

2.1.1 What is ERP System?

ERP (Enterprise Resource Planning) is an integrated computer-based system used to manage internal and external resources, including tangible assets, financial resources, materials, and human resources. Its purpose is to facilitate the flow of information between all business functions inside the boundaries of the organization and manage the connections to outside stakeholders. Built on a centralized database and normally utilizing a common computing platform, ERP systems consolidate all business operations into a uniform and enterprise-wide system environment.

An ERP system can either reside on a centralized server or be distributed across modular hardware and software units that provide "services" and communicate on a local area network. The distributed design allows a business to assemble modules from different vendors without the need for the placement of multiple copies of complex and expensive computer systems in areas which will not use their full capacity.

To be considered an ERP system, a software package should have the following traits:

- Should be integrated and operate in real time with no periodic batch updates.
- All applications should access one database to prevent redundant data and multiple data definitions.
- All modules should have the same look and feel.
- Users should be able to access any information in the system without needing integration work on the part of the IS department.

2.1.2 Components / Modules of an ERP Software:

- Transactional Backbone
    - Financials
    - Distribution
    - Human Resources
    - Product lifecycle management

- Advanced Applications
    - Customer Relationship Management (CRM)
    - Supply chain management software
        - Purchasing
        - Manufacturing
        - Distribution
    - Warehouse Management System

- Management Portal/Dashboard
    - Decision Support System

In a Bank, the following modules may be useful:

- Human Resources Management (HRM)
- Customer Relationship Management (CRM)
- Supply chain management
    - Purchasing
    - Distribution
- Warehouse Management (Asset Management)

2.1.3. Components of an ERP System

a) Manufacturing:

Engineering, bills of material, work orders, scheduling, capacity, workflow management, quality control, cost management, manufacturing process, manufacturing projects, manufacturing flow.

b) Supply chain management:

Order to cash, inventory, order entry, purchasing, product configurator, supply chain planning, supplier scheduling, inspection of goods, claim processing, commission calculation

c) Financials:

General ledger, cash management, accounts payable, accounts receivable, fixed assets

d) Project management:

Costing, billing, time and expense, performance units, activity management

e) Human resources:

Human resources, payroll, training, time and attendance, rostering, benefits

f) Customer relationship management:

Sales and marketing, commissions, service, customer contact, call-center support

g) Data services:

Various "self-service" interfaces for customers, suppliers and/or employees

h) Access control:

Management of user privileges for various processes

2.1.4. ERP advantages and disadvantages

Advantages

- Allows easier global integration (barriers of currency exchange rates, language, and culture can be bridged automatically)
- Updates only need to be done once to implemented company-wide
- Provides real-time information, reducing the possibility of redundancy errors
- May create a more efficient work environment for employees
- Vendors have past knowledge and expertise on how to best build and implement a system

Disadvantages

- Locked into relationship by contract and manageability with vendor - a contract can hold a company to the vendor until it expires and it can be unprofitable to switch vendors if switching costs are too high
- Inflexibility - vendor packages may not fit a company's business model exactly and customization can be expensive
- Return on Investment may take too long to be profitable
- Implementations have a risk of project failure

2.1.5. Renowned ERP Software:

2.1.5.1. SAP ERP from SAP

SAP (Systems Analysis and Program development) is a German software corporation that provides enterprise software applications and support to businesses of all sizes globally. Headquartered in Walldorf, Germany, with regional offices around the world, SAP is the largest enterprise software company in the world (as of 2009). It is also the largest software company in Europe and the fourth largest globally. The company's best known products are its SAP Enterprise Resource Planning (**SAP ERP**) and SAP Business Objects software.

The **SAP ERP** application is an integrated enterprise resource planning (ERP) software manufactured by SAP AG that targets business software requirements of midsize and large organizations in all industries and sectors. It allows for open communication within and between all company functions.

SAP's ERP solution includes several modules that support key functional areas, including:

- SAP ERP Financials
- SAP ERP Operations
- SAP ERP Human Capital Management

2.1.5.2. PeopleSoft ERP from Oracle

Oracle Corporation is an American multinational computer technology corporation that specializes in developing and marketing enterprise software products — particularly database management systems. Headquartered in Redwood Shores, California, United States, Oracle employs 105,000 people worldwide as of 1 July 2010. It has enlarged its share of the software market through organic growth and through a number of high-profile acquisitions. By 2007 Oracle had the third-largest software revenue, after Microsoft and IBM.

The corporation has arguably become best-known for its flagship product, the Oracle Database. The company also builds tools for database development and systems of middle-tier software, enterprise resource planning software (ERP), customer relationship management software (CRM) and supply chain management (SCM) software.

As of 2010, Larry Ellison, a co-founder of Oracle Corporation, has served as Oracle's CEO throughout its history. Ellison also served as the Chairman of the Board until his replacement by Jeffrey O. Henley in 2004. Ellison retains his role as CEO. On August 22, 2008 the Associated Press ranked founder Larry Ellison as the top-paid chief executive in the world.

PeopleSoft, Inc. was a company that provided human resource management systems (HRMS) and customer relationship management (CRM) software, as well as software solutions for manufacturing, financials, enterprise performance management, and student administration to large corporations, governments, and organizations. It existed as an independent corporation until its acquisition by Oracle Corporation in 2005. The PeopleSoft name and product line are now marketed by Oracle.

History of PeopleSoft:

- 1987: PeopleSoft, Inc. founded by David Duffield and Ken Morris in Walnut Creek, CA, USA.
- 1988: PeopleSoft HRMS released.
- 1994: Public distribution of Distribution and Financials modules.
- 1995: Launch of Student Administration System.
- 1996: Releases Manufacturing
- 1996: Releases **PeopleSoft 6**, their first ERP package.
- 2005: Acquired by Oracle Corporation.
- 2009: PeopleSoft HCM 9.1 is released.(October 2009)
- 2009: PeopleSoft FMS 9.1 is released.(November 2009)

2.2. CRM Software

2.2.1. What is CRM?

CRM (Customer relationship management) is a widely-implemented strategy for managing a company's interactions with customers, clients and sales prospects. It involves using technology to organize, automate, and synchronize business processes—principally sales activities, but also those for marketing, customer service, and technical support.

The overall goals are to find, attract, and win **new clients**, nurture and retain those the company already has, entice former clients back into the fold, and reduce the costs of marketing and client service. Customer relationship management describes a company-wide business strategy including customer-interface departments as well as other departments

The three phases in which CRM support the relationship between a business and its customers are to:

- Acquire: CRM can help a business acquire new customers through contact management, selling, and fulfillment.

- Enhance: web-enabled CRM combined with customer service tools offers customers service from a team of sales and service specialists, which offers customers the convenience of one-stop shopping.

- Retain: CRM software and databases enable a business to identify and reward its loyal customers and further develop its targeted marketing and relationship marketing initiatives

2.2.2. Fields of application:

2.2.2.1. Sales force automation

Sales force automation (SFA) involves using software to streamline all phases of the sales process, minimizing the time that sales representatives need to spend on each phase. This allows sales representatives to pursue more clients in a shorter amount of time than would otherwise be possible. At the heart of SFA is a contact management system for tracking and recording every stage in the sales process for each prospective client, from initial contact to final disposition. Many SFA applications also include insights into opportunities, territories, sales forecasts and workflow automation, quote generation, and product knowledge. Modules for Web 2.0 e-commerce and pricing are new, emerging interests in SFA.[1]

2.2.2.2. Marketing

CRM systems for marketing help the enterprise identify and target potential clients and generate leads for the sales team. A key marketing capability is tracking and measuring multichannel campaigns, including email, search, social media, telephone and direct mail. Metrics monitored include clicks, responses, leads, deals, and revenue. This has been superseded by marketing automation and Prospect Relationship Management (PRM) solutions which track customer behaviour and nurture them from first contact to sale, often cutting out the active sales process altogether.

2.2.2.3. Customer service and support

Recognizing that service is an important factor in attracting and retaining customers, organizations are increasingly turning to technology to help them improve their clients' experience while aiming to increase efficiency and minimize costs. Even so, a 2009 study revealed that only 39% of corporate executives believe their employees have the right tools and authority to solve client problems. The core for these applications has been and still is comprehensive call center solutions, including such features as intelligent call routing, computer telephone integration (CTI), and escalation capabilities.

2.2.2.4. Analytics

Relevant analytics capabilities are often interwoven into applications for sales, marketing, and service. These features can be complemented and augmented with links to separate, purpose-built applications for analytics and business intelligence. Sales analytics let companies monitor and understand client actions and preferences, through sales forecasting and data quality.

Marketing applications generally come with predictive analytics to improve segmentation and targeting, and features for measuring the effectiveness of online, offline, and search marketing campaign. Web analytics have evolved significantly from their starting point of merely tracking mouse clicks on Web sites. By evaluating "buy signals," marketers can see which prospects are most likely to transact and also identify those who are bogged down in a sales process and need assistance. Marketing and finance personnel also use analytics to assess the value of multi-faceted programs as a whole.

These types of analytics are increasing in popularity as companies demand greater visibility into the performance of call centers and other service and support channels,[6] in order to correct problems before they affect satisfaction levels. Support-focused applications typically include dashboards similar to those for sales, plus capabilities to measure and analyze response times, service quality, agent performance, and the frequency of various issues.

2.2.2.5. Integrated/Collaborative

Departments within enterprises — especially large enterprises — tend to function with little collaboration. More recently, the development and adoption of these tools and services have fostered greater fluidity and cooperation among sales, service, and marketing. This finds expression in the concept of collaborative systems which uses technology to build bridges between departments. For example, feedback from a technical support center can enlighten marketers about specific services and product features clients are asking for. Reps, in their turn, want to be able to pursue these opportunities without the burden of re-entering records and contact data into a separate SFA system. Owing to these factors, many of the top-rated and most popular products come as integrated suites.

2.2.3. Software for CRM

SAP, Oracle, Salesforce.com, Microsoft and Amdocs are the best selling software, according to the Gartner (www.gartner.com).

2.3. E-mail software

2.3.1. What is e-mail?

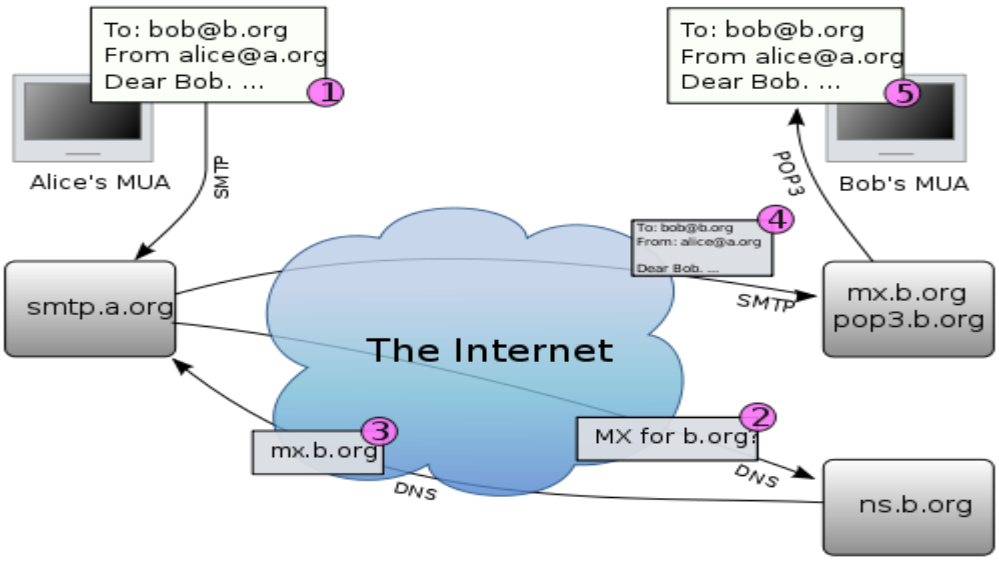
Electronic mail, commonly called email or e-mail, is a method of exchanging digital messages across the Internet or other computer networks.

In the manual systems of sending mail within an office, the mails are passed through persons from one department to another. It takes mush time and it is risky also .This leads the inconsistency of information. So we need a system which is both quick and accurate. This can be achieved by mailing system.

Electronic mailing system sends the mails spontaneously without requiring the parties be available at the same instant. Furthermore mails can be send to more people at the same time. It also leaves a written copy of the sending mails that can be filed away. It is much cheaper than the manual system.

2.3.2. Operation Overview:

The diagram below shows a typical sequence of events that takes place when Alice composes a message using her mail user agent (MUA). She enters the email address of her correspondent, and hits the "send" button.



1. Alice's MUA formats the message in email format and uses the Simple Mail Transfer Protocol (SMTP) to send the message to the local mail transfer agent (MTA), in this case smtp.a.org, run by Alice's internet service provider (ISP).

2. The MTA looks at the destination address provided in the SMTP protocol (not from the message header), in this case bob@b.org. An Internet email address is a string of the form localpart@exampledomain. The part before the @ sign is the *local part* of the address, often the username of the recipient, and the part after the @ sign is a domain name or a fully qualified domain name. The MTA resolves a domain name to determine the fully qualified domain name of the mail exchange server in the Domain Name System (DNS).

3. The DNS server for the b.org domain, ns.b.org, responds with any MX records listing the mail exchange servers for that domain, in this case mx.b.org, a server run by Bob's ISP.

4. smtp.a.org sends the message to mx.b.org using SMTP, which delivers it to the mailbox of the user bob.

5. Bob presses the "get mail" button in his MUA, which picks up the message using the Post Office Protocol (POP3).

2.3.3. Components in a messaging system:

E-mail Architecture addresses those technologies used to enable the electronic delivery of messages and documents to one or more recipients. The following provides a list of open source and commercially available software for use as different components like Mail Transfer Agents, Mail User Agents and Gateways:

1. Mail Transfer Agents:
    A. Open Source: Sendmail E-mail Application Server
    Qmail E-mail Application Server

    B. Commercial: MS Exchange E-mail Application Server
    Lotus Domino E-mail Application Server

2. Mail User Agents:
    A. Commercial: Lotus Notes E-mail Client
    Outlook E-mail Client
    Outlook Express E-mail Client
    Eudora E-mail Client

3. Gateways:
    A. Commercial: Lotus Message Switch E-mail Gateway
    Outlook Web Access E-mail Gateway

2.3.4. Popular E-mail System:

2.3.4.1. Sendmail:

Sendmail is a general purpose internetwork email routing facility that supports many kinds of mail-transfer and -delivery methods, including the Simple Mail Transfer Protocol (SMTP) used for email transport over the Internet.

2.3.4.2. Qmail:.

qmail is a mail transfer agent (MTA) that runs on Unix. It was written, starting December 1995, by Daniel J. Bernstein as a more secure replacement for the popular Sendmail program. qmail's source code is in the public domain, making qmail free software.

2.3.4.3. Microsoft Exchange Server:

Microsoft Exchange Server is the server side of a client–server, collaborative application product developed by Microsoft. It is part of the Microsoft Servers line of server products and is used by enterprises using Microsoft infrastructure products. Exchange's major features consist of electronic mail, calendaring, contacts and tasks; support for mobile and web-based access to information; and support for data storage.

2.3.4.4. Lotus Domino:

IBM Lotus Domino software is a world class platform for critical business, collaboration, and messaging applications.

2.3.5. Licensing of commercial product:

2.3.5.1. Exchange Server:

Exchange Server is licensed in the Server / Client Access License (CAL) model. A license must be assigned for each instance of the server software that is being run. Exchange also requires a CAL for each user or device that accesses the server software. There are two types of CALs for Exchange:

- **Standard CAL:** designed to help users be more productive from virtually any platform, browser, or mobile device, with new features in Exchange Server 2010 that help manage communications overload and lower helpdesk costs.

- **Enterprise CAL:** designed to allow organizations to reduce the costs and complexity of meeting compliance requirements with new integrated archiving functionality and information protection capabilities, while also helping users cut costs by replacing legacy voice mail systems with Unified Messaging.

Users also require license for Server Software, Microsoft Outlook and Forefront Online Security.

2.3.5.2. Lotus Domino:

IBM offers users three ways to license IBM Lotus Notes and Domino software to match their buying preferences and let them pay according to the function and flexibility they need.

If users prefer client and server licensing, they can acquire IBM Lotus Domino server licenses determined by the total processor value units associated with their server machine(s) plus individual Client Access Licenses for each user.

If users prefer per user licensing, they pay a per user charge based on the size of their environment, and have the flexibility to deploy any combination of specified types of IBM Lotus Domino server and client access options.

If users wish to host collaborative applications for access both outside and inside their company, but do not need mail and calendar, processor value unit licensing may be the most cost effective for them.

In both cases, if users are willing to deploy additional component like email security appliance, then this will add additional licensing cost to the overall system.

2.4. Anti-Virus software

2.4.1. What is antivirus software?

Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. You can help protect your computer against viruses by using antivirus software.

Computer viruses are software programs that are deliberately designed to interfere with computer operation, record, corrupt, or delete data, or spread themselves to other computers and throughout the Internet.

In the past, PCs were mainly under threat from viruses and worms. The main purpose of these programs was to spread; however, some programs were also designed to cause damage to files and PCs. Such malicious software, or “malware”, could be described as ‘cyber vandalism’. In the majority of cases, the goal of viruses and worms was to spread as much as possible, with a high infection rate leading to fame for that program.

But in recent years, the situation has changed drastically. Today, the biggest threat faced by computers is crime ware. This malicious software is written by cybercriminals with the purpose

of making money illegally. Crime ware may take the form of viruses, worms, Trojans or other malicious programs.

To help prevent the most current viruses, we must update our antivirus software regularly. Now a day, we can set up most types of antivirus software to update automatically.

2.4.2. How Antivirus works?

Antivirus uses number of techniques to identify viruses.

2.4.2.1. Signature based detection:

This is also known as dictionary approach. Each virus has its own way of attack. Signatures of the attacks are stored in antivirus database. To identify viruses, antivirus software compares the contents of a file to a dictionary of virus signatures. If a piece of code in the file matches any virus identified in the dictionary, the anti-virus software can then either delete the file, quarantine it so that the file is inaccessible to other programs and its virus is unable to spread, or attempt to repair the file by removing the virus itself from the file. For signature based detection antivirus software need to be updated with current virus signature database. Antivirus can take update from internet or by installing latest patches provided by the antivirus company.

2.4.2.2. Behavior Based Detection:

Antivirus identifies abnormal or unusual behavior (anomalies) on a host or PC. The basic idea comes from the assumption that attacks are different from “normal” (legitimate) activity of a file and therefore detect intrusions by identifying these differences. If one program tries to write data to an executable program, for example, this is flagged as suspicious behavior and the user is alerted to this, and asked what to do.

Antivirus can be installed and maintained only on client PC and take updates from internet. Moreover in LAN environment antivirus clients are installed on client PCs and managed from server-end. For this case server takes update from internet and distribute updates to client PCs.

2.4.3. Licensing:

Most of the commercial antivirus software end-user license agreements include one year subscription. User is asked for renewal 30 to 60 days before the license expiration. Purchasers provide bill for new license and get new activation code or serial number from the antivirus company. Antivirus fails to update the virus signature database if license is not renewed and computer security becomes compromised against new attack. Some antivirus programs are free to download but not effective as other commercial antivirus.

2.4.4. Popular Antivirus programs:

There are number of popular antiviruses available in the market such as Mcafee, Kaspersky, NOD32, Avsat, AVG etc. Some antivirus companies provide web security, email security, desktop management, PC solution, IDS (Intrusion Detection System), firewall as part of antivirus software package. For example, Kaspersky antivirus comes up with firewall and email security. Sometimes extra subscription fee is charged for each new module added to the antivirus software.

2.5. Anti-malware software

Malware is designed to cause damage to a stand-alone computer or a PC in a network. So wherever a malware term is used it means a program which is designed to damage a computer system - it may be a virus, worm or Trojan.

Virus is a program that embeds itself in some other executable software (including the operating system itself) on the target system without the user's consent and when that is run causes the virus to spread to other executable.

Warm is a stand-alone malware program that *actively* transmits itself over a network to infect other computers.

Trojans generally do not attempt to inject themselves into other files or otherwise propagate themselves. It misrepresents itself to appear useful, routine, or interesting in order to persuade a victim to install it

Anti-malware software is a type of software program created to protect computer systems from malicious software, or malware. Anti-malware programs scan a computer system to prevent, detect and remove malware.

Antivirus software is designed to detect and remove viruses and other malicious software from a system, whereas anti-malware software is a program that safeguards the system from all sorts of malware, including Virus, Trojans and worms.

McAfee, Norton, Kaspersky, Webroot, Avast, Trend Micro are the commercially available anti-malware software.

Review Questions

1. Multiple Choice Questions (MCQ)

i) Which of the following is not an instrument cleared through a clearing house?
a) Cheque b)Pay Order c) Dividend d) Gift Voucher

ii) Which of the following is not a part of clearing system?
a) RTGS b) BACH c) BACPS d) ERP

iii) Which of the following is not a component of an ERP system?
a) Manufacturing b) Supply Chain Management c) Human Resources d) Credit Card

iv) Which of the following is not an e-mail system?
a) Sendmail b) Lotus Domino c) Active-Passive Server d) Microsoft Exchange Server

2. Fill in the gap(s)

i) BACPS stands for ------ and BEFTN stands for --------

ii) BACPS was launched by the Bangladesh Bank in -----

iii) At presnt, ----- number of clearing systems are operating in Bangladesh

iv) The first clearing starts at ----- and the returns of the same occur at -------.

v) MICR stands for ---------

vi) The major MICR fonts used around the world are ---- and -----

vii) For clearing purpose, Bangladesh Bank provided all Banks a software called -----

Probable Questions

1. What is a Cheque Processing System?

2. Name four clearing systems that are in operation in Bangladesh.

3. Narrate the conventional cheque clearing process.

4. Define MICR, Cheque Truncation and RTGS.

5. What is BACH? What are the two parts of BACH? Narrate them.

6. What is a large value cheque settlement? How this is different than the normal cheque settlement?

7. What are the current timing in force for different clearing systems?

8. How MICR differs from a bar code?

9. How cheque truncation helps to stop physical movement of cheque?

10. What is PBM or participating Bank module in clearing system?

11. What are the benefits of a cheque truncation system over a traditional cheque clearing system?

12. What is the basic difference between RTGS and BEFTN?

13. What is routing number? What are the significance of digits of a routing number?

14. Why ERP software is used in banks?

15. Name a few components or modules of an ERP system.

16. Name two renowned commercial ERP software. Who are manufacturer of them?

17. Why a CRP software is used in a bank?

18. Brief in short the fields of application of a CRM software.

19. Narrate the importance of an email software.

20. Narrate in brief the four commercially used email systems?

21. Write the licensing policy of Exchange Server or Lotus Domino.

22. What is the difference between Virous and Malware? Name a few available Virus and Malware.

23. How an anti-virus software and an anti-malware software differs from each other?

24. Name five of each of the anti-virus software and an anti-malware software.

Module-F

FinTech
Artificial Intelligence
and future technology-based banking

1. FinTech, RegTech and TechFin

Interaction between banking and technology has a long history of mutual reinforcement and is much appreciated by the people associated with both. FinTech, RegTech and TechFin are some of these collaborations that have been successful so far with amazing innovative products.

1.1. FinTech

Financial technology (FinTech) is the technology and innovation that aims to compete with traditional financial methods in the delivery of financial services. The *FinTechs* are financial companies like Banks, Leasing companies, Insurance companies which embed FinTech to make their own products more attractive. Online Banking, Internet Banking, Debit Cards, Credit Cards, ATMs/CRMs, MFS, Agent Banking, mobile apps are the example of FinTech for banks. FinTech considerably improved services and the banks which adopted the FinTech first remain ahead of others in terms of growth.

The most well known solutions using FinTech in Bangladesh are NexusPay, ROCKET, bKash, Nagad, UPay, SSLCommerz, iFarmer, PayWell, Dmoney etc.

1.2 TechFin

The *TechFins* are technological companies, the main revenue of which comes from technological products and have acquired large amount of customer data from their core business, but now want to run a financial services based on the use of their customer's data. Examples of TechFin companies are social media company like Facebook, search engines like Google, e-commerce companies like Amazon, Telecommunication companies like Grameen Phone, Robi, Banglalink and hardware companies like IBM, Dell. They can use their data to price an insurance policy, to find prospective clients for a particular loan products or evaluate a customer's credit score.

Telecommunication companies in Bangladesh may want to start MFS for their own clients using their existing distribution channels or a neon loan product, client and amount of loan of which shall be determined based on the behavior of the use pattern, payment pattern of their network.

1.3 RegTech

Regulatory Technology popularly known as **RegTech**, is currently a buzzword in the global financial and compliance community. The term RegTech was first coined by the UK's Financial Conduct Authority (FCA) in 2015. According to their definition it's a subset of fintech that focuses on technologies that may facilitate the delivery of regulatory requirements more efficiently and effectively than existing capabilities.

In simple terms, it refers to any technology that ensures companies comply with their regulatory requirements. A perfect example of RegTech is the electronic Know Your Customer (eKYC) process by which banks verify the identities of the people who open new accounts digitally.

2. Basic Crypto Currency and Block Chain Technology

2.1 Block Chain Technology

A blockchain is a distributed database or ledger where data is stored electronically in digital format and shared among the nodes of a computer network. It is one of the most secured technology for storing data.

Blockchains are immutable and viewable to anyone of the network. It records data together in groups, known as block that has certain capacities of storing data. When a block is filled with data, is closed with hash including timestamps and are linked with previously filled blocks and generates a new hash. All new data are added in same manner, thus the formed blockchains make it immutable from deleting, altering or destroying any blocks in between the chains. This is how the blockchain technology becomes irreversible.

There are two types of blockchain network i.e. public network and private network of blockchain. The former has decentralized nodes distributed among public network and every member of the network can view the data, has anonymous user, no regulations or control over transaction but the data is immutable; and the latter has centralized nodes in private network where data is private, more control over transaction but is less secured.

Though this technology was first outlined in a research paper in 1991 but its' first real-world application was launched in January 2009, with the launch of Bitcoin. For its nature of record keeping, transactions and records in the blockchain technology in public network is irreversible i.e. records cannot be altered, deleted or destroyed, for which this technology is also known as distributed ledger technology (DLT).

By learning about blockchains, we foresee that industries having a requirement of stringent control over data i.e. immutable nature of data used in banking & finance, currency, insurance, stock market, remittance, property records, healthcare, supply chains, voting system etc. will incline to have blockchain technology in future. Currently cryptocurrency is leading user of blockchain technology.

In the context of Bangladesh, this technology can be used at nationwide level to manage the nationwide financial networks of Banks & NBFIs with decentralized nodes distributed among all of the Banks and NBFIs as a means of real-time transaction processing system, real-time BACH

processing etc. It can also be used to manage stock market with real-time data processing & settlement with decentralized nodes distributed among the various stakeholders of stock exchange including banks and the listed companies to update the stock holders in real-time. It can also be used to manage the nationwide MFSs to prevent customers' money from unauthorized use by others and to make a single network of MFS. Similarly, nationwide healthcare, public procurement, property records management and so on can also use the blockchain technology to leverage the benefits of blockchain.

2.2 Basic Crypto Currency

2.2.1. Why Crypto-Currency?

Satoshi Nakamoto was not happy with t*he existing currency and the way it is being operated by the Central Banks (or State).* Friedrich von Hayek in his book "*Denationalisation of Money: The Argument Refined"*: a*dvocated for a complete free market in the production, distribution and management of money to end the monopoly of central banks.*

This is how the concept of Crypto-currency emerges and this is where we need to think of minimizing public concerns.

2.2.2. Who is Satoshi Nakamoto?

- He invented Bitcoin (in 2009), the first and most popular crypto-currency of the world, using block chain technology. Nakamoto is said to be a pseudonymous person, Japanese national, was in his late 30s, while he invented Bitcoin.
- Groups of amateur detectives have been trying to workout who he really is, but couldn't succeed as yet.
- He is estimated to have mined 1m bitcoins before disappearing in 2010.
- At a price of $19,000/Bitcoin (in Dec/17, now $6,500/Bitcoin), he was the owner of $19bn in 2017.

2.2.3. Crypto-Currency in Bangladesh:

No Crypto-currency is in production or mining in Bangladesh, However there is activities relating to its buying and selling.

Bangladesh Bank's (Central Bank of Bangladesh) directives on crypto-currencies:

Bangladesh Bank on 15 Sept, 2014 issued a notice which said:

- It has been noticed that some people are engaged in buying and selling of bitcoin
- Such transactions may violate Foreign Currency Regulation Rule, 1947
- Bitcoin is not a legal tender and not recognized by the Bangladesh Bank or the Country

- As such the people engaged in dealing with Bitcoin may face financial loss
- To avoid financial loss and lawful actions, all are requested to refrain from transacting or helping to transact Bitcoin

Again on 24 Dec, 2017 Bangladesh Bank noticied:

- It is learnt from the news media that various crypto-currencies such as Bitcoin, Ethereum, Ripple, Litecoin etc are being transacted in Bangladesh
- These crypto-currencies are not legal tender, so no financial claim can be established against them
- These are not recognized by the central bank or the government of Bangladesh
- Transacting online with unknown persons has risk to be associated with Money Laundering or Terrorist Financing
- All the citizen of the country are requested to avoid transaction with crypto-currencies

2.2.4. What is a Legal Tender?

An amount of currency to be issued by a Central Bank is backed mainly by Gold; and/or Government Securities (such as long term bonds, Treasury Bills) which in turn is backed by Government earnings like Tax, Duty and other Revenue.

Venezuela issued a crypto-currency called Petro which is backed by its oil reserve

2.2.5. Crypto-Currency in its present state in the world

- Many Crypto-currencies are in place such as Bitcoin, Ether, Litecoin, Monero, Dash, PonziCoin, Zcash, Carbon, Tether, Petro.
- They are Electronic version of Cash, not controlled by a Central Bank
- Has no geographical boundary
- Users don’t require any KYC
- No specific authority, thus no consumer protection and no AML/CFT reporting
- Value is not backed by any assets

Thus Crypto-currency has failed to become a currency. It is frequently used for:

- Buying drugs and other illegal goods
- Payment of Ransom, human trafficking money
- Payment to organized terrorist groups

2.2.6. How Crypto-currency works ?

Parties Involved in Crypto-currency are:

1. Miners
2. Users
3. Online wallet providers
4. Exchange companies

i) Mining – Mining is the process of production of Crypto-currency.

- Miners generate bitcoin, record and ensure integrity
- In return they become owner of the bitcoin generated and also get a small amount of fee
- The network is designed in such a way that at any competition, the mining will take 10 minutes to produce 1 Bitcoin and a maximum of 21m Bitcoin can be produced (will be ended in 2140)
- BitFirms is a mining company in Montreal and consumes huge electricity (equal to the consumption of a country like Austria).
- The company also invested a huge amount of money in building a huge Data Center and setting up large computers & equipment.
- The company made a revenue of $4.5bn in 2017.

To make the production process understand, say there is only one computer/miner (so no competition!) engaged in production of Crypto-currency in this world. Say the speed of the computer is 2 GHz and it takes 10 minutes to generate 1 bitcoin. As there is no competition, the miner will produce 1 bitcoin every 10 minutes.

Now in the world, say there are two computers/miners and say the speed of Computer-1 is 2 GHz and that of Computer-2 is 10 GHz. So computer-2 has 5 times more chance to win/produce a bitcoin (like lottery) than computer-2. So in 120 minutes, 12 bitcoins will be produced – 2 by miner-1 and 10 by miner-2.

If the number of computers/miners increased, there will be less chance to win. However, if the speed of calculation of complex algorithm is high, there is high chance to win.

ii) Crypto-Currency End Users

1. Clients (End Users) need to download a full copy of block chain software in their computers and store the transaction chains themselves.
2. They need to keep the respective Private Key in a secured place (Pen drive stick or computer hard disk with appropriate backup – if lost, no transaction is possible and bitcoins are lost)
3. To spend a bitcoin, the owner must know the corresponding private key and digitally sign the transaction. The network verifies the signature using the public key.

Howvere, the maintaining points # 1 & 2 is costly and inconvenient for the end users. To avoid this, end users take help of Online Wallet Providers.

iii) Online Wallet providers

- Online Wallet provider is a tech firm which store credentials and transaction history of their respective clients, thus clients don't need to download a full copy of block chain software and store by themselves (like a member of stock exchange).
- Users credentials to access fund are stored with the Providers, as such users must have full trust on the providers
- A malicious Provider or a beach in server security of the Provider may cause entrusted bitcoins to be stolen.

iv) Exchange Companies

Exchange companies are agents where bitcoins are traded in exchange of traditional currency (like agent of MFS company).

2.2.7. What is the solution?

It is very difficult:

1. To detect, investigate, prosecute and prevent the use of crypto-currencies
2. Freezing / seizing crypto assets
3. Tracking movement of fund
4. Making someone compelled to file STRs

Because all the persons / parties involved are anonymous and not traceable

If it can't be arrested, it will kill the legal wallets and physical currencies. Meantime, as reported, virtual credit card & debit cards are already issued and virtual asset ATMs are installed !!

Therefore it is better to accept the concept, and produce Digital Currencies by the central banks of the respective countries. This will kill the illegal virtual assets and will remove physical cash from the country.

IMF Chief Christine Lagarde said in her recent speech at a conference in Singapore (Reference : BBC (14 Nov, 2018)) said:

Central banks could issue digital money

She also said:

- I believe we should consider the possibility to issue digital currency
- There may be a role for the state to supply money to the digital economy
- The advantage is clear. Your payment would be immediate, safe, cheap and potentially semi-anonymous... And central banks would retain a sure footing in payments
- Central banks in Canada, China, Sweden and Uruguay are all seriously considering digital currency proposals
- A virtual currency issued by a central bank would be a liability of the state - as cash is - not of a private firm
- This would help consumers by making transactions safer and more common, and as a result cheaper.

2.2.8. Introduction of National Digital Currency (NDC):

i) In bitcoin, the miner is anonymous and they setup huge data center as business goal. In case of National Digital Currency, the central bank will be the sole miner.

ii) In the bitcoin, the users are anonymous while in the National Digital Currency, users are bank clients registered through e-KYC verification from Election Commission database.

iii) The Online Wallet Providers in bitcoin are anonymous parties (not controlled by any authority) while in case of National Digital Currency Commercial Banks will act as Online Wallet Providers.

iv) In case of bitcoin, the Exchnage Companies are hidden companies not controlled by any authority while in case of National Digital Currency, the Exchange Companies are not required if it is decided not to make the NDC exchangeable with taka, else money changers and/or MFS and Agent Banking agents can act as nominated agents to convert taka into NDC or vice versa.

3. Artificial Intelligence

Artificial Intelligence (AI) is intelligence demonstrated by machines with learning and problem-solving technique in terms of rationality and acting rationally. AI research has been defined as the field of study of intelligent agents, which refers to any system that perceives its environment and takes actions that maximize its chance of achieving its goals. This includes advanced web search engines, understanding human speech, self-driving cars, automated decision-making and competing at the highest level in strategic game systems.

The financial industry generates large amounts of data where the big data is available. The banking industry needs a powerful tool to collect, structure and store information. Many banking and financial institutions are using AI being served such things as create and leverage

best integrated dataset, improve customer experience, enhance risk management, improve data security, boost regulatory compliances etc.

We can divide the AI impact in banking from two perspectives:

From the Customers' perspective:

1. AI assisted Account Opening via a virtual assistant.
2. Biometrics (face/iris/voice/fingerprint recognition) for account identification, money transaction.
3. Giving a personalized experience to each of the customers.
4. Providing AI enabled secured banking facilities.

From the Bank's perspective:

1. Customer identification uniquely from multiple resources
2. Deciding on the eligibility of loans for customers using machine learning algorithms based on the relevant data and giving a financial limit.
3. Forgery detection and identifying suspicious behavior.
4. Finding out the services which are used most and offering them accordingly to the customers.
5. Monitoring tools for the management and bank employees service standards.
6. Generating summarized insight from a vast amount of raw banking data, which can help shape the banking strategy in the future.
7. Generating offer/packages/services for the customers based on the customers' usage data.
8. Geographical, socio-economic data for the customers.
9. Competitor analysis and taking strategic decisions to stand up among them in the market.
10. Finding out promising investment sectors to make profit.
11. Deep learning models can be quite useful for forecasting bank crises including inflation and currency crises.

4. Future Technology-based Banking

4.1 Virtual/Digital Banking

Virtual/Digital Banking refers to the act of accessing banking institutions and their functions online without having to make a physical appearance at the bank branches. This is possible by extensive use of technology in the banking.

Many of the banks in Bangladesh already have adopted part of virtual/digital banking services and most popular services are Internet banking, e-commerce solution, mobile apps. Other services like ATM/CRM, MFS and agent banking requires the customers to physically go to an establishment like booth, agent etc.

One of the major concerns of people regarding virtual/Digital banking is security. Banking on the internet can be scary to many because of scammers and hackers, that's why virtual banks should take extra precautions to ensure that their platforms are secure and fit for financial operations.

On the other hand, **Virtual/Digital Banks** is a bank which does not have any physical presence**.** Customers open account with a virtual bank online and perform all the transactions virtually. Call centers of the virtual bank will help the customers if they need any assistance.

4.2 Cloud Computing

Cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet ("the cloud"). Instead of buying, owning, and maintaining physical data centers and servers, we can access technology services, on an as-needed and pay-as-you-go basis.

Cloud computing is one of the most attractive and promising technologies for the banking sector. But as per the existing rule, the customer's data can't be located outside the country, the cloud couldn't be adopted by the banks specially for core banking solutions. However banks have widely adoping cloud computing for miscellaneous services like HR, Inventory, email.

Types of cloud computing:

- Business Process-as-a-Service (BPaaS),
- Infrastructure-as-a-Service (IaaS),
- Platforms-as-a-Service (PaaS),
- Software-as-a-Service (SaaS)

While the advantages of Cloud Banking are increased agility and innovation, low maintenance cost and reduced IT complexity and enhanced security, the challenges are:

- Regulations conflict between local regulatory guidelines and compliance rules of cloud banking
- Security & privacy threat, i.e., data compromise
- Hazard of Data migration from existing system to cloud, i.e. large volume of data, incompetent technicians, legacy software etc.
- Risk of endangering user data, due to outsourcing of the migration to cloud
- Human error and incompetence, especially in coding, migration, maintenance etc.

- Un-interrupted cross border Internet and high bandwidth

4.3 Internet of Things (IoT)

IoT describes the network of physical objects — "things" (mobile phone, electrical appliances, barcode sensors, traffic lights etc.) that are embedded with sensors, software, and other technological microprocessors for the purpose of connecting and exchanging data with other devices and systems through internet.

How does IoT works:

- Internet-connected devices gathers data
- Collected data is transmitted from the devices to a gathering point, i.e. data center, cloud etc.
- Data processing and analytics

Customers can access these data, if permission is granted, and perform some activities like apply remote command on the IoT enabled devices, get online MIS reports and perform customized analysis. IoT can also be used to enhance the banking experiences of the customers and bankers.

4.4 Machine Learning

When a computer is configured to learn on its own using historical data and information with the help of thousands of extensive statistical and mathematical models, this is referred to as machine learning. Robo-advisor for credit scoring and appropriate investment recommendations, Chatbot for engaging and efficient customer service etc. are most common machine learning based applications now-a-days.

Fraud detection, risk management, customers behavior analysis, purchase pattern and many other tasks at banks may be improved by use of machine learning. For example, if a cfedit card is used now in Bangladesh and then within half an hour it is used in USA, the system can detect this as a fraud transaction as, no customer will be able to go to USA from Bangladesh in half an hour time. Other use cases may be automating tasks, spotting fraud before it occurs, processing loans more quickly and accurately, enhancing the effectiveness of compliance checks.

The advantage of applying machine learning for banks is to reduce operational expenses and boost earnings. Machine learning will increase a company's competitiveness by giving it a major edge over its competitors. Additionally, by better comprehending how people spend their money, machine learning algorithms may provide better offers, discounts, and products that clients would desire to purchase or invest in.

4.5 Data Mining

One of the recent advancement in line with data management technologies is data mining and knowledge discovery. **Data mining** is the process of extracting and discovering patterns in large datasets involving methods at the intersection of machine learning, statistics, and database systems. Data has increased in size and dimensionality. Despite this, it is more frequently utilized in the sector as a tool to research clients and make best options.

Finding useful information from vast data repositories to address important business concerns is a technique known as data mining. This mountain of data that is being saved on a daily basis is evolving into the organization's most valuable asset. Data mining has enormous potential for use by banks in areas including marketing, credit risk management, money laundering detection, liquidity management, investment banking, and the timely detection of fraudulent transactions. A bank can detect fraud before it has an impact on its profitability by studying the patterns of its transactions. Data mining could be useful in achieving these highly desired qualities.

4.6 Data Warehouse

A system used for reporting and data analysis and is considered a core component of business intelligence. It's a one sort of central repositories of integrated data from one or more sources. For example, a bank may have various databases like core banking data, Retail loan data, SME loan data, credit card data, MFS data, ecommerce data and agent banking data. A data warehouse integrates all the data into one and arrange them using some key identifiers like customer number, mobile number or NID number. The some very important decisions are taken by the system and submit to the banking officials as reports.

With the help of analytics or reports, banks may segment their customer bases to increase profitability and be successful in attracting new clients. For banks, data warehouse services are frequently the answer to many more queries.

Therefore, in short, the data warehouses are the tools used by banks to address and manage the data that might help them better understand their clients' needs and take a closer look. When a corporation uses the appropriate data and analytics, it can distinguish between expansion and depletion. To achieve this knowledge, effective data management and analysis are essential. And this can be achieved by the use of data warehousing solution.

Some of the commercially available data warehousing solutions are: Teradata, Microsoft Azure, Amazon Redshift, BigQuery, SAP and SAS.

4.7 Current Trends

Massive transformation is happening in banking sector along with the technological advancement. Technology has become synonymous to business. Hence Banking Sector is evolving from traditional banking towards digital and Artificial Intelligence based. We adopted the blessings of technology since long which can be found in many aspects like Artificial Intelligence, Machine Learning, Algorithms, Block Chain, Crypto currency, IoT, 5G and many others.

Some of the major technologies which are being used currently by Banking Sector can be stated below:

- Customer Self on-boarding (E-KYC).
- Digital money (crypto currency) is being used which will reduce to use of physical currency.
- Financial Apps for doing any kind of transactions, fund transfer, enquiry balance/statements, E-payment, E-loan etc.
- Cardless ATM withdrawal, Deposit & Withdrawal using CRM
- QR and NFC payment.
- IVR (Interactive Voice Response) & Video Banking.
- E-commerce
- Finger-print, face detection, voice banking

Upcoming AI based Technologies in Banking Sector:

- Virtualization and cloud based banking with the help of block chain technology.
- Use of virtual and augmented reality.
- Personalization and Intelligence service using Machine learning, Data Science
- BaaS (Banking as a service), Paas(platform as a service) is going to be introduced.

Security will be one of the main concern to take advantage of digital banking properly. Strong cyber security, user identity, safeguarded device, location will be of higher priority.

Finally, transformation will be happened with the blessing of technology and to secure market share, banks will need to focus on the virtualization and digital banking very strongly.

Review Questions

1. Multiple Choice Questions (MCQ)

i) Which of the following is not a FinTech for Banks?

a) Credit Card b) ATM c) Q-Management d) Mobile Apps

ii) Which of the following is not a TechFins?

a) Facebook b) Amazon c) Dutch-Bangla Bank d) Grameen Phone

iii) Which of the following is not a party in Crypto-Currency production and processing?

a) Miners b) Central Bank c) Online Wallet Providers d) Exchange Companies

iv) Digital Banking has -----

a) a few branches b) no branches c) a few agents d) huge number of employees

2. Fill in the gap(s)

i) The FinTechs are financial companies like -----, ----- and ------ which embad FinTech to make their own products more attractive.

ii) Most well known solutions using FinTech in Bangladesh are ----, ----- and ---------

iii) ---------- refers to any te hnology that ensures companies comply with their regulatory requirements.

iv) ---------- invented Bitcoin in --------

v) Amount of currency to be issued by a central bank is backed mainly by ----------

vi) ---------- is the process of production of crypto-currency.

Probable Questions

1. What is the differences between FinTech and TechFin?

2. Name a few of the FinTech solutions in use in Bangladesh.

3. Is Grameen Phone a TechFin company? Why?

4. Define the following:

    RegTech, Virtual Banking, Cloud computing, Internet of Things, Machine learning, Data mining, Data Warehouse.

5. In which areas of banking, the block chain technology can be used?

6. Who is Satoshi Nakamoto? Why he dislikes existing currencies?

7. What is the status of Crypto-currency in Bangladesh?

8. What is the present state of Crypto-currency in the world?

9. How Crypto-currency works? Narrate in details.

10. How many parties are involved in Crypto-currency?

11. What is the role of a miner in Crypto-currency production?

12. Who are the Crypto-currency end users?

13. What are the functions of an Online Wallet Providers?

14. What the Exchange Companies do?

15. What it is difficult to control Crypto-currency?

16. State the idea of introducing National Digital Currency? How it is different than Crypto-currency?

17. What is Artificial Intelligence? How Artificial Intelligence impact the banking?

18. What are the advantages of cloud banking? What are the challenges?

19. Describe current trend in banking in respect to technology use.

References

1. Abul Kashem Md. Shirin and Nusrat Tamanna Prianka (2020): “Information Technology in Financial Services” 2nd Ed., The Institute of Bankers, Bangladesh (IBB)”.

2. Carol V. Brown, Daniel W DeHyes, Jeffrey Slater, Waingaert E. Martin: “Managing Information Technology”.

3. C.S. French, 1990: “Computer Studies, 3rd ed., Arnold Publishers, New Delhi, India”.

4. Graham Taylor, 2001: “GCSE Computer Studies, 4th ed., Macmillan Press Ltd., London”.

5. Grau, J. J. (ed.), 1992: “Criminal and Civil Investigation Handbook, 2nd ed., McGraw-Hill Inc., New York”.

6. Harry Bouwman, Bart Van den Hooff, Lidwein van de Wijngaert, Jan van Dijk: “Information and Communication Technology in Organizations”.

7. Indian Institute of Banking (IIB): “Electronic Banking and Information Technology”.

8. James A. O’Brien, 1999: “Management Information Systems, 4th ed., Tata McGraw-Hill Publishing Company Limited, New Delhi, India”.

9. Kenneth C. Laudon & Jane P. Laudon, 1999: “Management Information Systems – Organization and Technology, 4th ed., Prentice Hall of India, New Delhi – 110 001”.

10. Pete Loshin & Paul A. Murphy, 1999: “Electronic Commerce, 2nd ed., Jaico Publishing House, Mumbai, India”.

11. Wikipedia, 2010: “Wikipedia, the free encyclopedia on the internet on www.en.wikipedia.org/wiki/”.

12. Yekini Nureni: “Information Communication Technology (ICT)”.

About Author

Abul Kashem Md. Shirin is the Managing Director & CEO of Dutch-Bangla Bank Limited (DBBL). He joined DBBL as Executive Vice President and head of IT in 2003. Under his leadership, DBBL has established a largest ATM Network, a POS network, first e-commerce Payment Gateway (Nexus Gateway), first Chip-based EMV Credit and Debit Cards (Nexus Cards), first mobile Financial Service (rocket) of the country and a bio-metric based Agent Banking operation in Bangladesh.

He was the first Deputy Managing Director (DMD) in the Banking sector of the country from IT background. He is also the first Managing Director in a bank in Bangladesh having Engineering background.

Before joining DBBL, he worked in the BASIC bank as Deputy General Manager and head of IT, and the Bangladesh Sugar and Food Industries Corporation as Computer programmer and Thakurgaon Sugar Mills as Assistant Engineer.

Mr. Shirin obtained his M. Engg.degree in Computer Science and Engineering from Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh. He also obtained his educations from Sunamgonj Jubilee High School, Sylhet M.C. College, Bangladesh Agricultural University, Mymensingh and Asian Institute of Technology (AIT), Bangkok, Thailand.

He is also the author of a book named “Computer Programming” published by the Bangla Academy in 1998. The book was a best seller one and was very famous among young programmers and students of MBA, BBA, B.Sc. Ag. Engg, Diploma in Computer Science and Electronics, HSC, SSC, and A & O Level.