CHAPTER 5

CORE BANKING SYSTEMS

LEARNING OUTCOMES

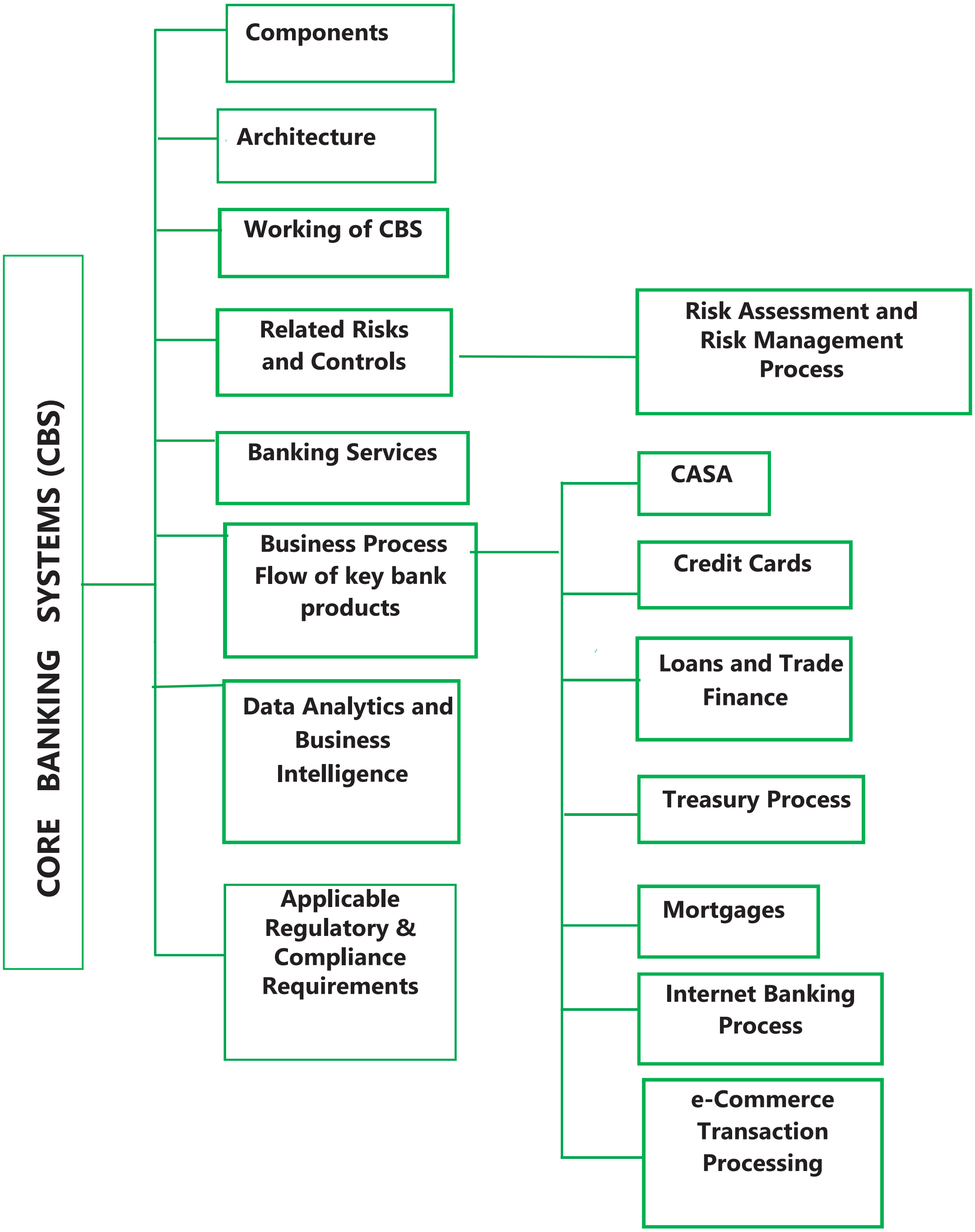
After reading this chapter, you will be able to -

❑ Understand components and architecture of CBS and impact of related risks and controls.

❑ Appreciate the functioning of core modules of banking and business process flow and impact of related risks and controls.

❑ Comprehend regulatory and compliance requirements applicable to CBS such as Banking Regulations Act, RBI regulations, Prevention of Money Laundering Act and Information Technology Act.

CHAPTER OVERVIEW


CORE BANKING SYSTEMS (CBS)
Components
Architecture
Working of CBS
Related Risks and Controls
Risk Assessment and Risk Management Process
Banking Services
Business Process Flow of key bank products
CASA
Credit Cards
Loans and Trade Finance
Treasury Process
Mortgages
Internet Banking Process
e-Commerce Transaction Processing
Data Analytics and Business Intelligence
Applicable Regulatory & Compliance Requirements

5.1 OVERVIEW OF BANKING SERVICES

5.1.1 Introduction

Today India's banks compete at the world stage at one level and provide basic banking services to citizens of India staying at the remotest location in India. All this has been built over period of time and many factors have helped this happen.

Key factors that helped banks reach this level of service delivery being:

1. Information Technology (IT) is an integral aspect of functioning of enterprises and professionals in this digital age. This has now made banking services increasingly digital with IT plays a very critical role. The rapid strides in IT and the rapid adoption of technology by banks have empowered banks to use it extensively to offer newer products and services to its customers.

2. India as a country could not let behind from global business opportunities. Ushering of reforms by successive governments led to huge growth in India's global business. Customers also sought banks to provide services that enabled them to compete in global economy as well as create new business opportunities in India. As business grew so the need of customer also grew.

3. Successive governments focus to have financial inclusion for all Indians. Banks were found to be most capable of helping government achieve this goal.

4. Growth of internet penetration across India.

To be able to meet the requirements of its customers, to be able to meet the global challenges in banking and to enhance its service delivery models banks in India adopted **CORE BANKING SYSTEMS (CBS)**. CBS are centralized systems allowing banks to scale up operations, better service delivery and improved customer satisfaction.

Banking is the engine of economic growth specifically in a rapidly developing country like India with its diverse background, practices, cultures and large geographic dispersion of citizens. Banking has played a vital and significant role in the development of the economy. The changes in the banking scenario due to moving over to Core Banking System and IT-based operations have enabled banks to reach customers and facilitate seamless transactions with lesser dependence on physical infrastructure. This has resulted in all the core functions at the branches, such as loan processing and sanctioning, safe keeping of security documents, post sanction monitoring and supervision of borrower's accounts, accounting of day-to-day transactions, receipts and payments of cash/cheques and updating passbooks/statements, being either centralized or made online or with the use of ATMs. The accounting transactions and all services of the banks are being done from a central server using core banking solutions. This is changing the modus operandi of how banking services are delivered to customers by using alternate delivery channels such as ATM, Internet Banking and Mobile Banking.

5.1.2 Overview of Banking Services

The core of banking functions is acceptance of deposits and lending of money. Further, specific services such as demand drafts, bank guarantees, letter of credits, etc. are also provided. The key features of a banking business are as follows:

- The custody of large volumes of monetary items, including cash and negotiable instruments, whose physical security should be ensured.
- Dealing in large volume (in number, value and variety) of transactions.
- Operating through a wide network of branches and departments, which are geographically dispersed.
- Increased possibility of frauds as banks directly deal with money making it mandatory for banks to provide multi-point authentication checks and the highest level of information security.

Some of the major products and services provided and rendered by commercial banks which constitute core banking services are briefly explained here in the Fig 5.1.1.

I. Acceptance of Deposits

Deposits involve deposits by customers in various schemes for pre-defined periods. Deposits fuel the growth of banking operations; this is the most important function of a commercial bank. Commercial banks accept deposits in various forms such as term deposits, savings bank deposits, current account deposits, recurring deposits and various other innovative products like saving-cum-term deposits, flexi-deposit accounts and various others products.

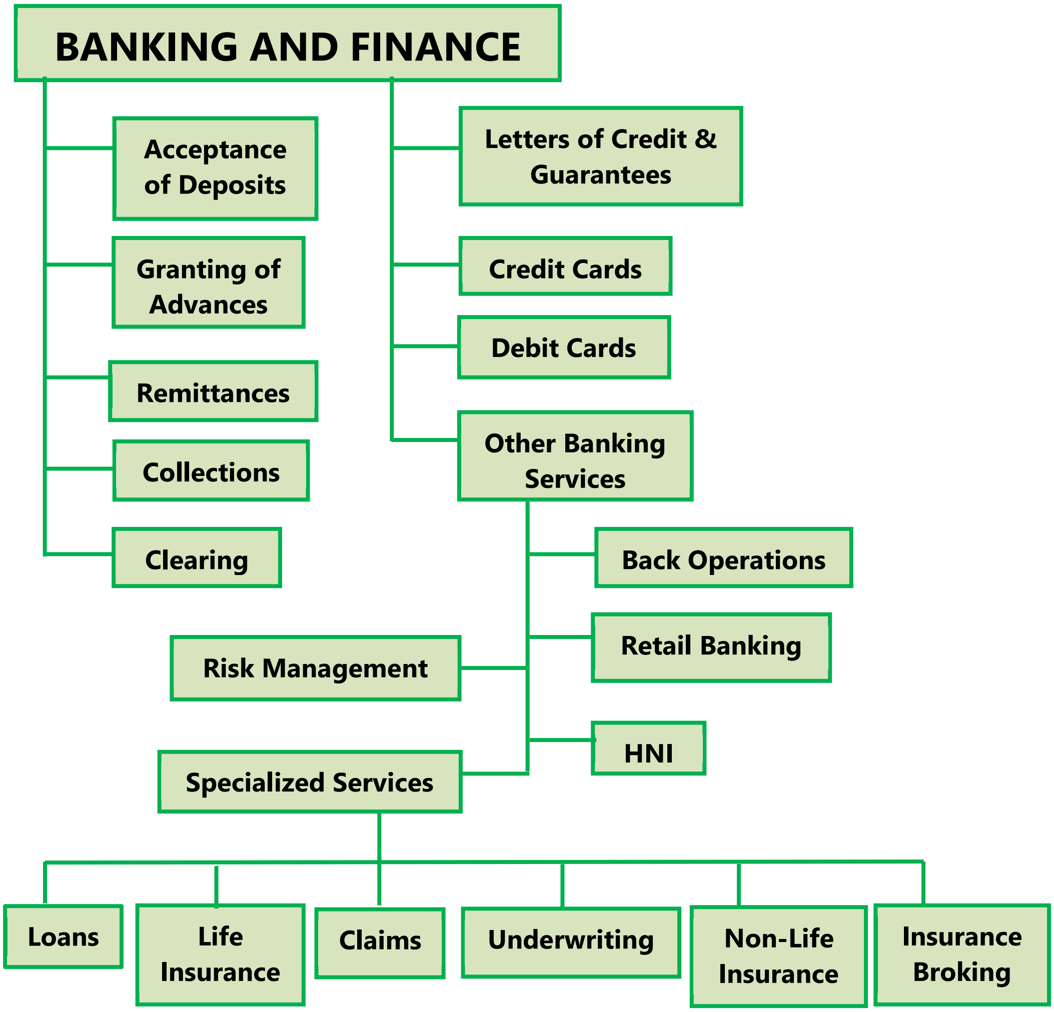


Fig. 5.1.1: Banking and Finance Services

II. Granting of Advances

Advances constitute a major source of lending by commercial banks. The type of advances granted by commercial banks take various forms such as cash credit, overdrafts, purchase/ discounting of bills, term loans, etc. Apart from granting traditional facilities, banks also provide facilities like issuance of commercial papers, ECB (External Commercial Borrowing) on behalf of bank/borrower, securitization of credit sales, housing loans, educational loans, and car loans, etc. An external ECB is an instrument used in India to facilitate the access to foreign money by Indian corporations and public sector undertakings.

In rural areas, banks have become a major channel for disbursement of loans under various government initiatives like KCC (Kisan Credit Cards), Mudra Yozana, and many such social welfare schemes run by state and central governments across India.

III. Remittances

Remittances involve transfer of funds from one place to another. Two of the most common modes of remittance of funds are demand drafts and Telegraphic Transfers/Mail Transfers (TT/ MT). Drafts are issued by one branch of the Bank and are payable by another branch of the Bank (or, in case there being no branch of the Bank at the place of destination, branch of another Bank with which the issuing Bank has necessary arrangements). The drafts are handed over to the applicant. In the case of telegraphic/ mail transfer, no instrument is handed over to the applicant; the transmission of the instrument is the responsibility of the branch. Generally, the payee of both the TT and the MT is an account holder of the paying branch. Electronic Funds Transfer is another mode of remittance which facilitates almost instantaneous transfer of funds between two centers electronically. Most of the banks have now introduced digital mode of remittance which makes remittance possible online and on mobile devices directly by the customer in a few clicks. In recent times, new modes of money transfer have replaced the traditional methods of funds transfer. These include:

(a) **Real Time Gross Settlement (RTGS)** is an electronic form of funds transfer where the transmission takes place on a real-time basis. In India, transfer of funds with RTGS is done for high value transactions, the minimum amount being ₹ 2 lakh. The beneficiary account receives the funds transferred, on a real- time basis.

(b) **National Electronic Funds Transfer (NEFT)** is a nation-wide payment system facilitating one-to-one funds transfer. Under this Scheme, individuals can electronically transfer funds from any **bank** branch to any individual having an account with any other **bank** branch in the country participating in the Scheme.

(c) **Immediate Payment Service (IMPS)** is an instant payment inter-**bank** electronic funds transfer system in India. **IMPS** offers an inter-**bank** electronic fund transfer service through mobile phones. Unlike NEFT and RTGS, the service is available 24/7 throughout the year including **bank** holidays.

IV. Collections

Collections involve collecting proceeds on behalf of the customer. Customers can lodge various instruments such as cheques, drafts, pay orders, travelers' cheques, dividend and interest warrants, tax refund orders, etc. drawn in their favor and the trade bills drawn by them on their buyers with their Bank for collection of the amount from the drawee (the bank or the drawee of the bill). They can also lodge their term deposit receipts and other similar instruments with the Bank for collection of the proceeds from the Bank with which the term deposit, etc. is maintained. Banks also collect instruments issued by post offices, like national savings certificates, postal orders, etc.

With increased access to internet and banks having created large branch networks through CBS, banks have upgraded their collections services. Now both public and private sector banks provide cash as well as cheque collection services for its customers. Banks provide these services for pre-defined destinations, time and locations and on call basis. For these services banks charges a nominal collections fees.

V. Clearing

Clearing involves collecting instruments on behalf of customers of bank. The instruments mentioned above may be payable locally or at an outside center. The instruments payable locally are collected through clearing house mechanism, while the instruments payable outside is sent by the Bank with whom the instrument has been lodged, for collection to the branches of the issuing Bank at those centers or, if there is no such branch, to other banks. Clearing house settles the inter-Bank transactions among the local participating member banks. Generally, post offices are also members of the house. There may be separate clearing houses for MICR (Magnetic Ink Character Recognition) and non-MICR instruments. MICR is a technology which allows machines to read and process cheques enabling thousands of cheque transactions in a short time. MICR code is usually a nine-digit code comprising of some important information about the transaction and the bank.

Electronic Clearing Services (ECS) is used extensively now for clearing. ECS takes two forms: **ECS Credit** or **ECS Debit**.

- In the case of **ECS credit**, there is a single receiver of funds from large number of customers, e.g. public utilities, mutual funds, etc. The beneficiary (i.e., the receiver of funds) obtains mandate from its customers to withdraw funds from their specified Bank accounts on a specific date.

- In the case of **ECS debit**, there is a single account to be debited against which many accounts with number of banks in the same clearing house area are credited. This system is useful for distribution of dividend/ interest, payment of salaries by large units, etc.

The Bank/ Branches, who have adopted Core Banking System (CBS) honor instruments even of other branches beyond their clearing zone payable at par by the designated branch of that center. This system facilitates easy payment mechanism from any center particularly. This facility is now available to most customers of the bank.

VI. Letters of Credit and Guarantees

Issuing letters of credit and guarantees are two important services rendered by banks to customers engaged in business, industrial and commercial activities. A **Letter of Credit (LC)** is an undertaking by a bank to the payee (the supplier of goods and/ or services) to pay to him, on behalf of the applicant (the buyer) any amount up to the limit specified in the LC, provided the terms and conditions mentioned in the LC are complied with. The **Guarantees** are required by the customers of banks for submission to the buyers of their goods/ services to guarantee the performance of contractual obligations undertaken by them or satisfactory performance of goods supplied by them, or for submission to certain departments like excise and customs, electricity boards, or to suppliers of goods, etc. in lieu of the stipulated security deposit.

VII. Credit Cards

The processing of applications for issuance of credit cards is usually entrusted to a separate division at the central office of a bank. The dues against credit cards are collected by specified branches. Many of them also act as 'cash points’ to provide cash to the cardholder on demand up to the specified limits. Most credit cards issued by banks are linked to one of the international credit card networks like VISA, Master, Amex or India’s own RuPay which currently issues debit cards but credit cards are also expected to be launched in near future.

VIII. Debit Cards

Debit Cards are issued by the bank where customer is having their account. Debit cards are generally issued by the central office of the bank. Debit Cards facilitates customers to pay at any authorized outlet as well as to withdraw money from an ATM from their account. Debit cards are networked with an inter-bank network. When a debit card is used for a transaction, the amount is immediately deducted from the customer's account balance.

IX. Other Banking Services

The Fig. 5.1.1 gives an overview of complete range of various types of banking services. The key type of transactions related to banking activities have been explained here. Some of the key terms used in the figure are further explained here.

- **Back operations:** These cover all operations done at the back office of the bank. These are related to general ledger, Management Information Systems, reporting, etc.
- **Retail Banking:** These are also called front-office operations that cover all operations which provide direct retail services to customers.
- **High Net-worth Individuals (HNI):** Banks provide special services to customers classified as High Net-worth Individuals (HNI) based on value/ volume of deposits/ transactions.
- **Risk Management:** Risks are all pervasive in the banking sector. This should be done at strategic, tactical, operational and technology areas of the bank. Risk management is best driven as per policy with detailed standards, procedures and guidelines provided for uniform implementation.
- **Specialized Services:** Banks also perform other services such as loan, insurance broking, claims, underwriting, life insurance, non-life insurance, etc. However, these would be offered by separate entities set up by the bank.
    - o **Loan:** A loan is money, property or other material goods given to another party in exchange for future repayment of the loan value amount, along with interest or other finance charges. A loan may be for a specific, one-time amount or can be available as an open-ended line of credit up to a specified limit or ceiling amount.

- **Underwriting:** Underwriting is the process that banks and other financial institutions use to assess the credit worthiness or risk of a potential borrower. During this stage of the loan process, the underwriter checks the borrower's ability to repay the loan based on an analysis of his/her credit history, collateral, and capacity. Underwriting typically happens behind the scenes, but it is a crucial aspect of loan approvals.

- **Life Insurance:** Life Insurance can be defined as a contract between an insurance policy holder and an insurance company, where the insurer promises to pay a sum of money in exchange for a premium, upon the death of an insured person or after a set period.

Note: The Fig. 5.1.1 includes some non-banking services such as claims, insurance, etc. which may be done by the bank or an independent subsidiary. All banks may not carry all given services as these are not core banking activities. Some services such as insurance, underwriting, etc. may be done through separate subsidiaries.

5.1.3 Overview of Core Banking Systems (CBS)

Core Banking Solution (CBS) refers to a common IT solution wherein a central shared database supports the entire banking application. The characteristics of CBS are:

- There is a common database in a central server located at a Data Center, which gives a consolidated view of the bank's operations.

- Branches function as delivery channels providing services to its customers.

- CBS is centralized Banking Application software that has several components which have been designed to meet the demands of the banking industry.

- CBS is supported by advanced technology infrastructure and has high standards of business functionality.

- Core Banking Solution brings significant benefits such as a customer is a customer of the bank and not only of the branch.

- CBS is modular in structure and is capable of being implemented in stages as per requirements of the bank.

- A CBS software also enables integration of all third-party applications, including in-house banking software, to facilitate simple and complex business processes.

Some examples of CBS software are given below. These are only illustrative and not exhaustive.

- **Finacle:** Core banking software suite developed by Infosys that provides universal banking functionality covering all modules for banks covering all banking services.
- **FinnOne:** Web-based global banking product designed to support banks and financial solution companies in dealing with assets, liabilities, core financial accounting and customer service.
- **Flexcube:** Comprehensive, integrated, interoperable, and modular solution that enables banks to manage evolving customer expectations.
- **BaNCS:** A customer-centric business model which offers simplified operations comprising loans, deposits, wealth management, digital channels and risk and compliance components.
- **bankMate:** A full-scale Banking solution which is a scalable, integrated e-banking systems that meets the deployment requirements in traditional and non-traditional banking environments. It enables communication through any touch point to provide full access to provide complete range of banking services with anytime, anywhere paradigm.

Further, there are many CBS software developed by vendors which are used by smaller and co-operative banks. Some of the banks have also developed in-house CBS software. However, the trend is for using high-end CBS developed by vendors depending on cost-benefit analysis and needs.

Core Banking Solution has become a mandatory requirement to provide a range of services demanded by customers and the competitive banking environment. This requires that most of bank’s branches access applications from centralized data centers. CBS for a bank functions not only as a heart (circulatory system) but also as a nervous system. All transactions flow through these core systems, which, at an absolute minimum, must remain running and responsive during business hours. These systems are usually running 24x7 to support Internet banking, global operations, and real time transactions via ATM, Internet, mobile banking, etc.

Key modules of CBS are given in the Fig. 5.1.2:

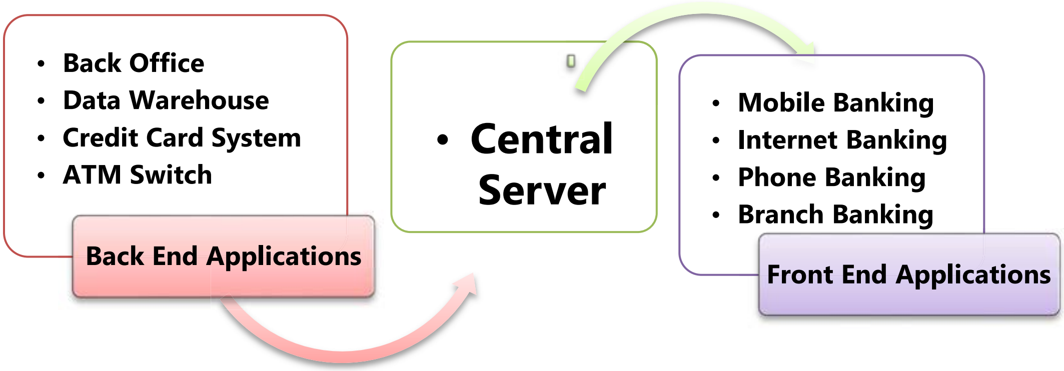


Fig. 5.1.2: Key Modules of CBS

(The Front End and Back End Applications discussed in Chapter 2)

Fig. 5.1.2 is a simple diagram illustrating how most of the key modules of bank are connected to a common central server. In the case of a CBS, at the core is Central server. All key modules of banking such as back office, branch, data warehouse, ATM Switch, mobile banking, internet banking, phone banking and credit-card system are all connected and related transactions are interfaced with the central server ad are explained below:

- ***<u>Back Office:</u> The Back Office is the portion of a company made up of administration and support personnel, who are not client-facing. Back-office functions include settlements, clearances, record maintenance, regulatory compliance, accounting, and IT services. Back Office professionals may also work in areas like monitoring employees' conversations and making sure they are not trading forbidden securities on their own accounts.***

- ***<u>Data Warehouse:</u> Banking professionals use data warehouses to simplify and standardize the way they gather data - and finally get to one clear version of the truth. Data warehouses take care of the difficult data management - digesting large quantities of data and ensuring accuracy - and make it easier for professionals to analyze data.***

- ***<u>Credit-Card System:</u> Credit card system provides customer management, credit card management, account management, customer information management and general ledger functions; provides the online transaction authorization and service of the bank card in each transaction channel of the issuing bank; Support in the payment***

application; and at the same time, the system has a flexible parameter system, complex organization support mechanism and product factory based design concept to speed up product time to market.

- ***<u>Automated Teller Machines (ATM):</u> An Automated Teller Machine (ATM) is an electronic banking outlet that allows customers to complete basic transactions without the aid of a branch representative or teller. Anyone with a credit card or debit card can access most ATMs. ATMs are convenient, allowing consumers to perform quick, self-serve transactions from everyday banking like deposits and withdrawals to more complex transactions like bill payments and transfers.***

- ***<u>Central Server:</u> Initially, it used to take at least a day for a transaction to get reflected in the real account because each branch had their local servers, and the data from the server in each branch was sent in a batch to the servers in the data center only at the end of the day (EOD). However, nowadays, most banks use core banking applications to support their operations creating a Centralized Online Real-time Exchange (or Environment) (CORE). This means that all the bank's branches access applications from centralized data centers/servers, therefore, any deposits made in any branch are reflected immediately and customer can withdraw money from any other branch throughout the world.***

- ***<u>Mobile Banking & Internet Banking:</u> Mobile Banking and Internet banking are two sides of the same coin. The screens have changes, the sizes have become smaller and banking has become simpler. Mobile banking is a much latest entrant into the digital world of banking.***

    - ***<u>Internet Banking</u> also known as Online Banking, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website. The online banking system offers over 250+ services and facilities that give us real-time access to our bank account. We can make and receive payments to our bank accounts, open Fixed and Recurring Deposits, view account details, request a cheque book and a lot more, while you are online.***

    - ***<u>Mobile Banking</u> is a service provided by a bank or other financial that allows its customers to conduct financial institution that allows its customers to conduct financial transactions remotely using a mobile device such as a Smartphone or tablet. Unlike the***

related internet banking, it uses software, usually called an app, provided by the financial institution for the purpose. Mobile banking is usually available on a 24-hour basis.

- ***<u>Phone Banking:</u> It is a functionality through which customers can execute many of the banking transactional services through Contact Centre of a bank over phone, without the need to visit a bank branch or ATM. Registration of Mobile number in account is one of the basic perquisite to avail Phone Banking. The use of telephone banking services, however, has been declining in favor of internet banking. Account related information, Cheque Book issue request, stop payment of cheque, Opening of Fixed deposit etc. are some of the services that can be availed under Phone Banking.***

- ***<u>Branch Banking:</u> CBS are the bank's centralized systems that are responsible for ensuring seamless workflow by automating the frontend and backend processes within a bank. CBS enables single-view of customer data across all branches in a bank and thus facilitate information across the delivery channels. The branch confines itself to the following key functions:***
    - ***Creating manual documents capturing data required for input into software;***
    - ***Internal authorization;***
    - ***Initiating Beginning-Of-Day (BOD) operations;***
    - ***End-Of-Day (EOD) operations; and***
    - ***Reviewing reports for control and error correction.***

To conclude, CBS implementation has cut down time, working at the same time on dissimilar issues and escalating usefulness. The platform where communication technology and information technology are merged to suit core needs of banking is known as core banking solutions. Here, computer software is used to perform core operations of banking like recording of transactions, passbook maintenance, and interest calculations on loans & deposits, customer records, balance of payments and withdrawal. Normal core banking functions will include deposit accounts, loans, mortgages and payments. Banks make these services available across multiple channels like ATMs, Internet banking, and branches.

5.1.4 Core features of CBS

Banking industry is involved in dealing with public money and thus demands proper checks and balances to ensure close monitoring of the dealing, minimizing the risk arising out of the banking business.

A CBS is built with these inherent features. In the past few years, banks have implemented these major technology initiatives and have deployed new state-of-the-art and innovative banking services. One of the significant projects implemented is the Centralized Database and Centralized Application Environment for core and allied applications and services which is popularly known as CBS. The design and implementation of CBS has been completed in most of the commercial banks.

In addition to basic banking services that a bank provides through use of CBS, the technology enables banks to add following features to its service delivery.

- On-line real-time processing.
- Transactions are posted immediately.
- All databases updated simultaneously.
- Centralized Operations (All transactions are stored in one common database/server).
- Separate hierarchy for business and operations.
- Business and Services are productized.
- Remote interaction with customers.
- Reliance on transaction balancing.
- Highly dependent system-based controls.
- Authorizations occur within the application.
- Increased access by staff at various levels based on authorization.
- Daily, half yearly and annual closing,
- Automatic processing of standing instructions,
- Centralized interest applications for all accounts and account types
- Anytime, anywhere access to customers and vendors.

5.2 COMPONENTS AND ARCHITECTURE OF CBS

5.2.1 Technology Components of CBS

The software resides in a centralized application server which is in the Central Office Data Centre, so the application software is not available at the branch but can be accessed from the branches or online. Along with database servers and other servers, an application server is located at the Central Data Centre. The CBS deployed by the Banks as a part of the CBS Project includes Data Centre (DC) and the Disaster Recovery Centre (DRC).

The key technology components of CBS are as follows:

- Database Environment
- Application Environment
- Web Environment
- Security Solution
- Connectivity to the Corporate Network and the Internet
- Data Centre and Disaster Recovery Centre
- Network Solution architecture to provide total connectivity
- Enterprise Security architecture
- Branch and Delivery channel
- Online Transaction monitoring for fraud risk management

Some key aspects in-built into architecture of a CBS are as follows:

- **Information flow:** This facilitates information flow within the bank and improves the speed and accuracy of decision-making. It deploys systems that streamline integration and unite corporate information to create a comprehensive analytical infrastructure.
- **Customer centric:** Through a holistic core banking architecture, this enables banks to target customers with the right offers at the right time with the right channel to increase profitability.
- **Regulatory compliance:** This holds the compliance in case bank is complex and expensive. CBS has built-in and regularly updated regulatory platform which will ensure compliance.

- **Resource optimization:** This optimizes utilization of information and resources of banks and lowers costs through improved asset reusability, faster turnaround times, faster processing and increased accuracy.

5.2.2 CBS IT Environment

The Fig. 5.2.1 provides an overview of CBS IT Environment with client access devices at the top which interface with channel servers which in turn interface with application servers which are connected to the database servers hosted on windows/Unix platform. CBS is a Technology environment based on Client-Server Architecture, having a Remote Server (called Data Centre) and Client (called Service Outlets which are connected through channel servers) branches. The Server is a sophisticated computer that accepts service requests from different machines called Clients. The requests are processed by the server and sent back to the clients.

These concepts are further explained below.

A. Application Server

All the transactions of the customer are processed by the data center. The **Application Server** performs necessary operations and this update the account of the customer 'A' in the database server. The customer may do some other operation in branch "Y". The process is validated at branch "Y" and the data is transmitted to the application software at the data center. The results are updated in the database server at the centralized data center. Thus, it would be observed that whatever operations a customer may do at any of the branches of the bank the accounting process being centralized at the centralized data center is updated at the centralized database.

B. Database Server

The **Database Server** of the Bank contains the entire data of the Bank. The data would consist of various accounts of the customers and master data (e.g., of master data are customer data, employee data, base rates for advances, FD rates, the rate for loans, penalty to be levied under different circumstances, etc.). Application software would access the database server.

C. Automated Teller Machines (ATM) Channel Server

This server contains the details of ATM account holders. Soon after the facility of using the ATM is created by the Bank, the details of such customers are loaded on to the ATM server. When the Central Database is busy with central end-of- day activities or for any other reason, the file containing the account balance of the customer is sent to the ATM switch. Such a file is called Positive Balance File (PBF). This ensures not only continuity of ATM operations but also ensures that the Central database is always up-to-date. The above process is applicable to stand alone ATMs at the Branch level. As most of the ATMs are attached to the central network, the only control is through ATM Switch.

D. Internet Banking Channel Server (IBCS)

Just as in the case of ATM servers, where the details of all the account holders who have ATM facility are stored, the Internet Banking database server stores the user name and passwords of all the internet banking customers. **IBCS (Internet Banking Channel Server)** software stores the name and password of the entire internet banking customers. Please note that the ATM server does not hold the PIN numbers of the ATM account holders. IBCS server also contains the details about the branch to which the customer belongs. The Internet Banking customer would first have to log into the bank's website with the user name and password.

E. Internet Banking Application Server

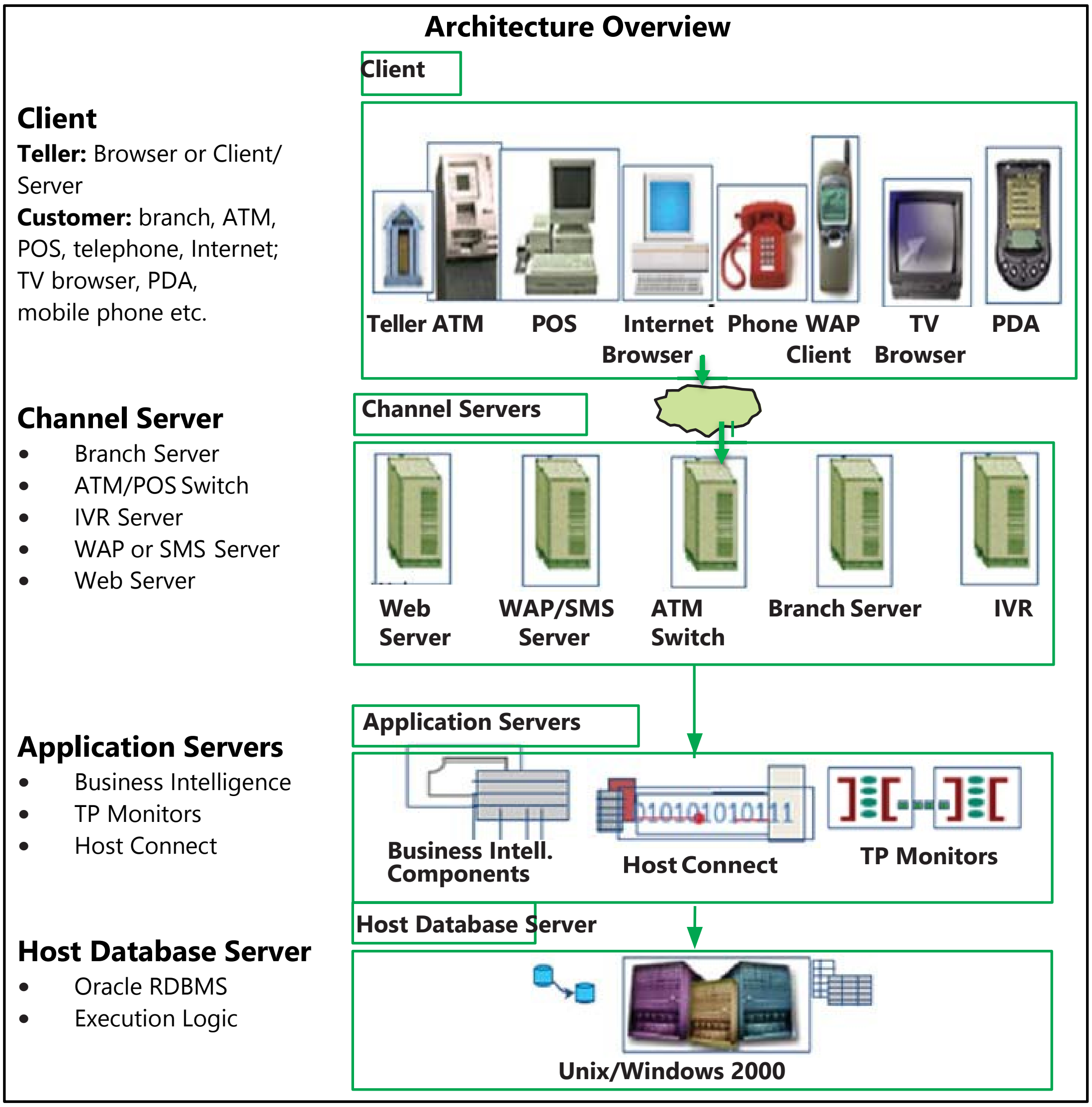
The **Internet Banking Software** which is stored in the IBAS (Internet Banking Application Server) authenticates the customer with the login details stored in the IBCS. Authentication process is the method by which the details provided by the customer are compared with the data already stored in the data server to make sure that the customer is genuine and has been provided with internet banking facilities.

F. Web Server

The **Web Server** is used to host all web services and internet related software. All the online requests and websites are hosted and serviced through the web server. A Web server is a program that uses HTTP (Hypertext Transfer Protocol) to serve the files that form Web pages to users, in response to their requests, which are forwarded by their computers' HTTP clients. Dedicated computers and appliances may be referred to as Web servers as well. All computers that host Web sites must have Web server programs.

G. Proxy Server

A **Proxy Server** is a computer that offers a computer network service to allow clients to make indirect network connections to other network services. A client connects to the proxy server, and then requests a connection, file, or other resource available on a different server. The proxy provides the resource either by connecting to the specified server or by serving it from a cache. In some cases, the proxy may alter the client's request or the server's response for various purposes.



Client

Teller: Browser or Client/ Server

Customer: branch, ATM, POS, telephone, Internet; TV browser, PDA, mobile phone etc.

Channel Server

- Branch Server
- ATM/POS Switch
- IVR Server
- WAP or SMS Server
- Web Server

Application Servers

- Business Intelligence
- TP Monitors
- Host Connect

Host Database Server

- Oracle RDBMS
- Execution Logic

Fig. 5.2.1: CBS IT Environment

H. Anti-Virus Software Server

The **Anti-Virus Server** is used to host anti-virus software which is deployed for ensuring all the software deployed are first scanned to ensure that appropriate virus/ malware scans are performed.

5.2.3 Functional Architecture of CBS

A Core Banking Solution is the enterprise resource planning software of a bank. It covers all aspects of banking operations from a macro to micro perspective and covers the entire gamut of banking services ranging from front office to back office operations, transactions at counters to online transactions up to general ledger and reporting as required. However, a CBS is modular in nature and is generally implemented for all functions or for core functions as decided by the bank. For example, if treasury operations or foreign exchange transactions are minimal, then this may not be implemented in CBS but the results could be linked to CBS as linked with the proper interface. Hence, the implementation would depend on the need and criticality of specific banking services provided by the bank. The following Fig. 5.2.2 provides a functional architecture of CBS covering the complete range of banking services.

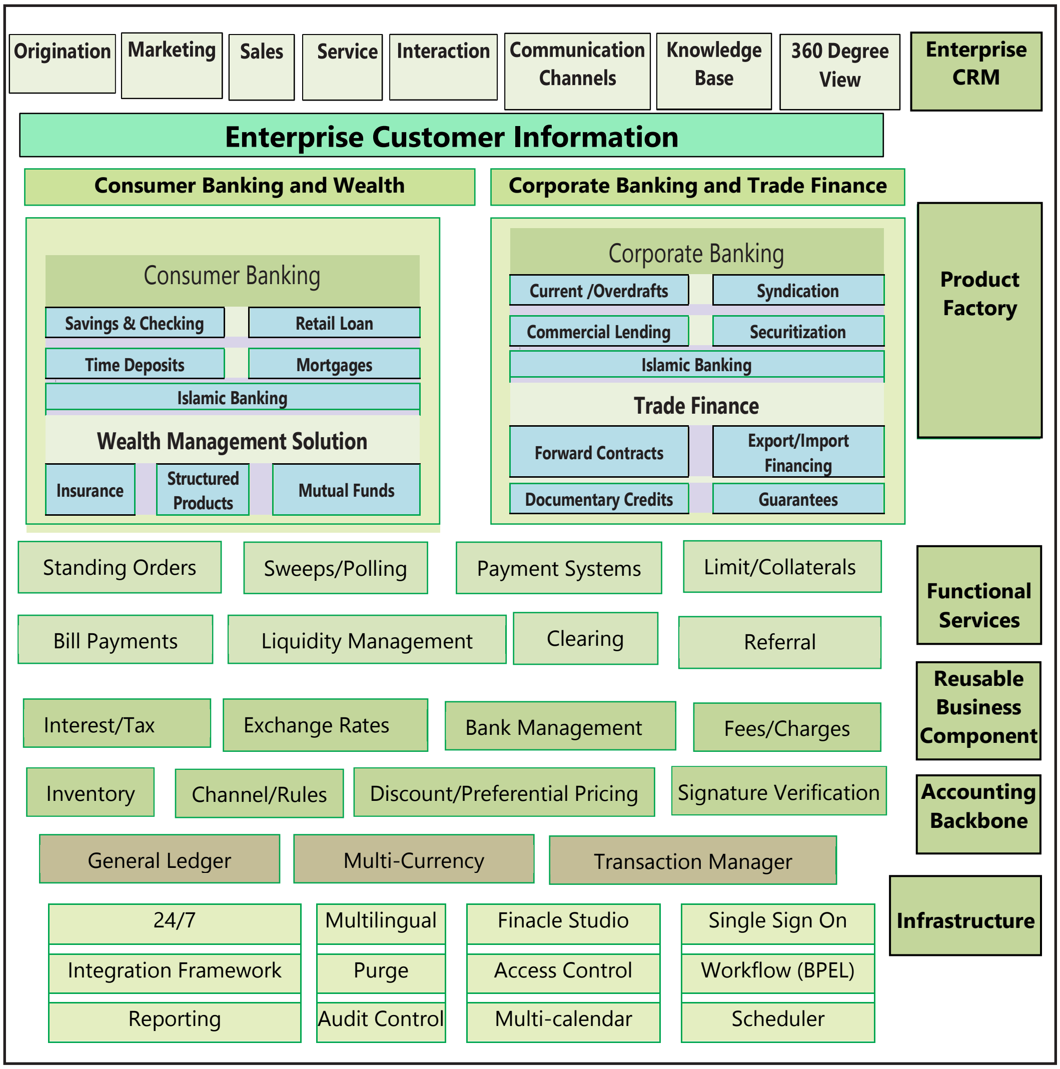


Fig. 5.2.2: Functional Architecture of CBS[1] (Illustrative)

[1] Source: Finacle

5.2.4 Internet Banking Process

- The customer applies to the bank for such a facility. The user is provided with a User ID and Password. As is the best practice the password is expected to be changed soon after the first log on.
- Internet facility could be used only by accessing the website of the bank. For accessing the website, naturally a browser like Internet Explorer, Firefox or Chrome is used.
- On access, user is directed to secure web server. The internet banking website is hosted on the web server. The web server is in the central data centre of the bank. Access to the web server is permitted only to authorized users.
- To protect the web server from unauthorized use and abuse, the traffic is necessarily to go past a firewall. The firewall is designed in such a fashion that only traffic addressed to the web server through the authorized port is permitted.
- An individual who accesses the website of bank through the browser will be able to access the web server and there will be a display of the bank's web page on the screen of the client's computer.
- The web page will also provide all information generally of interest to the public. The web page also will have a specified area wherein a mention of user ID and password will be made.
- The password will not be displayed in plain text but will only be in an encrypted form.
- The web server forwards the customer details to the internet banking applications server which in turn accesses the IDBS. The server has already the database of all the customers who have been provided with internet banking facility. For each customer, it would be having details about user ID and password.
- The information received from the web server is verified with the data of the customer held in the internet banking (IBAS).
- Should the information not tally, the message 'access denied' would appear giving the reason giving the 'user ID/ password incorrect'. The customer realizing the mistake may rectify the mistake and make another attempt.
- Normally, three such attempts would be permitted. After three attempts, the customer will be logged out for security reasons. If more attempts are permitted, there is a possibility of a person just trying out different combination of user ID and password to break into the system.

- Based on the authentication check, the Internet Banking Application Server (IBAS) sends an acknowledgement to the web server. The web server displays the message. Once the authentication process is completed correctly, the customer is provided internet banking facility, which would include:

  (a) Password change

  (b) Balance inquiry

  (c) Fund transfer

  (d) Request for cheque book

  (e) Stop payment

  (f) Copy of statement of account; and

  (g) ATM/ Credit Card related queries

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

The customer would be able to get the service required e.g., viewing of the statement of account or a screen made available for him to request for a cheque book or instructions for 'stop payment' etc. After the services provided, the user may choose to log out. The customer may be permitted to request for more than one service in one session. Some software would automatically log out the customer after one service has been completed and expect users to log in again. It needs to be emphasized that security is a serious concern in internet banking and should be implemented with great care.

5.2.5 e-Commerce Transaction processing

Most of the e-Commerce transactions involve advance payment either through a credit or debit card issued by a bank. The Fig. 5.2.3 highlights flow of transaction when a customer buys online from vendor's e-commerce website. Here, the user logs in on the e-commerce web site, places an order and selects option of payment-Cards or Internet Banking.

If it is Internet Banking, the merchant site is directed to bank's Merchant-Internet banking server. User must log in and authorize payment. In India, this requires customer enter OTP (Online Transaction Password) received on mobile, to complete the transaction. After this, the customer is redirected to merchant site.

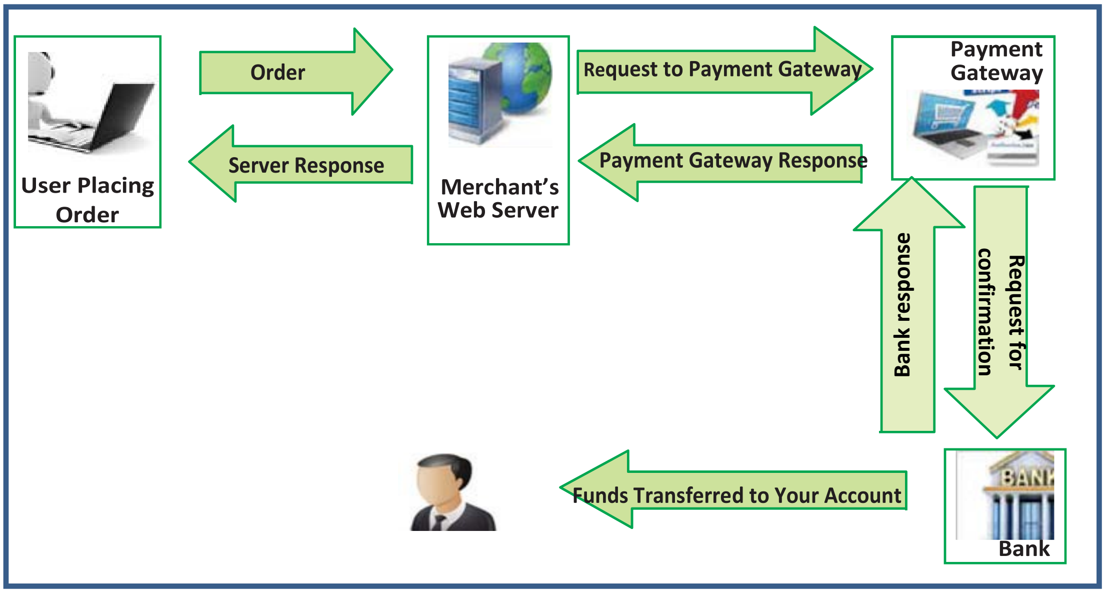


Fig. 5.2.3: e-Commerce Transaction flow for approval of payments

5.2.6 Case Study of IT deployment in Bank

XYZ Bank is one of the largest Public Sector Banks in India. Prosys is a leading Information technology company in India offering quality software products and services both in the domestic and international markets. The Bank has signed a strategic IT partnership with Prosys. Accordingly, XYZ Bank has licensed Prosys Banking software which includes Banksoft - the Core Banking Solution, eConnect - the Financial Middleware, and eBanker - the Internet Banking Solution. XYZ Bank intends to deploy Banksoft across 1500 branches over the next 3 years.

Solution: The IT solution to be deployed by the Bank envisages setting up of a data center with main server(s) (Web server, Database server and application server) and back up servers. The data center will be replicated at another location with similar type of hardware and network. The identified branches will be connected to the data center and the back-up data center through V-Sat and Lease lines. Each of the branches will have terminals with Windows QVT/Net Version for Telnet and I-Link Net/Win Version as interface for printing. XYZ Bank has 9500 ATMs which are connected to the main servers and it intends to add another 3000 ATMs which are to be located at different locations. Customers of any of the 12500 branches can operate their accounts and transact on-line from anywhere

5.2.7 Implementation of CBS

An automated information system such as CBS provides the platform for processing the information within the enterprise and extends to external service providers. The CBS software meets the needs of banks right from customers, staff, vendors, regulators and auditors. CBS covers the entire flow of information right from initiation, processing to storage and archiving of information. The CBS also interfaces with various type of software that may be developed in-house or procured from different vendors. This software must be updated as required on a regular basis. The deployment and implementation of CBS should be controlled at various stages to ensure that banks automation objectives are achieved:

- **Planning:** Planning for implementing the CBS should be done as per strategic and business objectives of bank.
- **Approval:** The decision to implement CBS requires high investment and recurring costs and will impact how banking services are provided by the bank. Hence, the decision must be approved by the board of directors.
- **Selection:** Although there are multiple vendors of CBS, each solution has key differentiators. Hence, bank should select the right solution considering various parameters as defined by the bank to meet their specific requirements and business objectives.
- **Design and develop or procured:** CBS solutions used to be earlier developed in-house by the bank. Currently, most of the CBS deployment are procured. There should be appropriate controls covering the design or development or procurement of CBS for the bank.
- **Testing:** Extensive testing must be done before the CBS is live. The testing is to be done at different phases at procurement stage to test suitability to data migration to ensure all existing data is correctly migrated and testing to confirm processing of various types of transactions of all modules produces the correct results.

- **Implementation:** CBS must be implemented as per pre-defined and agreed plan with specific project milestones to ensure successful implementation.
- **Maintenance:** CBS must be maintained as required. E.g. program bugs fixed, version changes implemented, etc.
- **Support:** CBS must be supported to ensure that it is working effectively.
- **Updation:** CBS modules must be updated based on requirements of business processes, technology updates and regulatory requirements;
- **Audit:** Audit of CBS must be done internally and externally as required to ensure that controls are working as envisaged.

5.3 CBS RISKS, SECURITY POLICY AND CONTROLS

5.3.1 Risks associated with CBS

(a) ***Operational Risk:*** ***It is defined as a risk arising from direct or indirect loss to the bank which could be associated with inadequate or failed internal process, people and systems. Operational risk necessarily excludes business risk and strategic risk. The components of operational risk include transaction processing risk, information security risk, legal risk, compliance risk and people risk.***

People risk arises from lack of trained key personnel, tampering of records, unauthorized access to dealing rooms and nexus between front and back end offices. Processing risk arises because faulty reporting of important market developments to the bank management may also occur due to errors in entry of data for subsequent bank computations. Legal Risk arises because of the treatment of clients, the sale of products, or business practices of a bank. There are countless examples of banks being taken to court by disgruntled corporate customers, who claim they were misled by advice given to them or business products sold. Contracts with customers may be disputed.

(b) ***Credit Risk:*** ***It is the risk that an asset or a loan becomes irrecoverable in the case of outright default, or the risk of an unexpected delay in the servicing of a loan. Since bank and borrower usually sign a loan contract, credit risk can be considered a form of counterparty risk.***

(c) ***Market Risk:*** ***Market risk refers to the risk of losses in the bank's trading book due to changes in equity prices, interest rates, credit spreads, foreign-exchange rates, commodity prices, and other indicators whose***

values are set in a public market. To manage market risk, banks deploy several highly sophisticated mathematical and statistical techniques

(d) ***Strategic Risk:*** ***Strategic risk, sometimes referred to as business risk, can be defined as the risk that earnings decline due to a changing business environment, for example new competitors or changing demand of customers.***

(e) ***Compliance Risk:*** ***Compliance risk is exposure to legal penalties, financial penalty and material loss an organization faces when it fails to act in accordance with industry laws and regulations, internal policies or prescribed best practices.***

(f) **IT Risk:** Once the complete business is captured by technology and processes are automated in CBS; the Data Centre (DC) of the bank, customers, management and staff are completely dependent on the DC. From a risk assessment and coverage point of view, it is critical to ensure that the Bank can impart advanced training to its permanent staff in the core areas of technology for effective and efficient technology management and in the event of outsourcing to take over the functions at a short notice at times of exigencies. Some of the common IT risks related to CBS are as follows:

- **Ownership of Data/ process:** Data resides at the Data Centre. Establish clear ownership.
- **Authorization process:** Anybody with access to the CBS, including the customer himself, can enter data directly. What is the authorization process? ***If the process is not robust, it can lead to unauthorized access to the customer information.***
- **Authentication procedures:** ***Usernames and Passwords, Personal Identification Number (PIN), One Time Password (OTP) are some of the most commonly used authentication methods.*** However, these may be inadequate and hence the user entering the transaction may not be determinable or traceable.
- **Several software interfaces across diverse networks:** A Data Centre can have as many as 75-100 different interfaces and application software. ***A data center must also contain adequate infrastructure, such as power distribution and supplemental power subsystems, including electrical switching; uninterruptable power supplies; backup generators and so on. Lapse in any of these may lead to real-time data loss.***

- o **Maintaining response time:** Maintaining the interfacing software and ensuring optimum response time and up time can be challenging.
- o **User Identity Management:** This could be a serious issue. Some Banks may have more than 5000 users interacting with the CBS at once.
- o **Access Controls:** Designing and monitoring access control is an extremely challenging task. ***Bank environments are subject to all types of attacks; thus, a strong access control system is a crucial part of a bank's overall security plan. Access control, however, does vary between branch networks and head office locations.***
- o **Incident handling procedures:** Incident handling procedures are used to address and manage the aftermath of a security breach or cyberattack. However, these at times, may not be adequate considering the need for real-time risk management.
- o **Change Management:** Though Change management reduces the risk that a new system or other change will be rejected by the users; however, at the same time, it requires changes at application level and data level of the database- Master files, transaction files and reporting software.

5.3.2 Security Policy

Large corporations like banks, financial institutions need to have a laid down framework for security with properly defined organizational structure. This helps banks create whole security structure with clearly defined roles, responsibilities within the organization. Banks deal in third party money and need to create a framework of security for its systems. This framework needs to be of global standards to create trust in customers in and outside India.

Information Security

Information security is critical to mitigate the risks of Information technology. Security refers to ensure Confidentiality, Integrity and Availability of information. RBI has suggested use of ISO 27001: 2013 implement information security. Banks are also advised to obtain ISO 27001 Certification. Many banks have obtained such certification for their data centers. Information security is comprised of the following sub-processes:

- **Information Security Policies, Procedures and practices:** Refers to the processes relating to approval and implementation of information security. The security policy is basis on which detailed procedures and practices are developed and implemented at various units/department and layers of technology, as relevant. These cover all key areas of securing information at various layers of information processing and ensure that information is made available safely and securely.

- **User Security Administration:** Refers to security for various users of information systems. The security administration policy documents define how users are created and granted access as per organization structure and access matrix. It also covers the complete administration of users right from creation to disabling of users is defined as part of security policy.
- **Application Security:** Refers to how security is implemented at various aspects of application right from configuration, setting of parameters and security for transactions through various application controls.
- **Database Security:** Refers to various aspects of implementing security for the database software.
- **Operating System Security:** Refers to security for operating system software which is installed in the servers and systems which are connected to the servers.
- **Network Security:** Refers to how security is provided at various layers of network and connectivity to the servers.
- **Physical Security:** Refers to security implemented through physical access controls.

Sample listing of Risks and Controls w.r.t Information Security is available in Table 5.3.1.

Table 5.3.1: Sample Listing of Risks and Controls w.r.t Information Security

Risks	Key IT Controls
Significant information resources may be modified inappropriately, disclosed without authorization, and/or unavailable when needed. (e.g., they may be deleted without authorization.)	Super user access or administrator passwords are changed on system, installation and are available with administrator only. Password of super use or administrator is adequately protected.
Lack of management direction and commitment to protect information assets.	Security policies are established and management monitors compliance with policies.
Potential Loss of confidentiality, availability and integrity of data and system.	Vendor default passwords for applications systems, operating system, databases, and network and

	communication software are appropriately modified, eliminated, or disabled.
User accountability is not established.	All users are required to have a unique user id.
It is easier for unauthorized users to guess the password of an authorized user and access the system and/or data. This may result in loss of confidentiality, availability and integrity of data and system.	The identity of users is authenticated to the systems through passwords. The password is periodically changed, kept confidential and complex (e.g., password length, alphanumeric content, etc.)
Unauthorized viewing, modification or copying of data and/ or unauthorized use, modification or denial of service in the system.	System owners authorize the nature and extent of user access privileges, and such privileges are periodically reviewed by system owners.
Security breaches may go undetected.	Access to sensitive data is logged and the logs are regularly reviewed by management.
Potential loss of confidentiality, availability and integrity of data and system	Physical access restrictions are implemented and administered to ensure that only authorized individuals can access or use information resources.
Inadequate preventive measure for key server and IT system in case of environmental threat like heat, humidity, fire, flood etc.	Environmental control like smoke detector, fire extinguisher, temperature maintenance devices and humidity control devices are installed and monitored in data center.
Unauthorized system or data access, loss and modification due to virus, worms and Trojans.	Network diagram is prepared and kept updated. Regular reviews of network security are performed to detect and mitigate network vulnerabilities.

5.3.3 Internal Control System in Banks

The objective of internal control system is to ensure orderly and efficient conduct of business, adherence to management policies, safeguarding assets through prevention and detection of fraud and error, ensuring accuracy and completeness of the accounting record and timely preparation of the reliable financial information. For example, Internal controls in banking would be to ensure that the transaction or decision are within the policy parameters laid down by the bank, they do not violate the instruction or policy prescription and are within delegated authority.

(a) Internal Controls in Banks

Risks are mitigated by implementing internal controls as appropriate to the business environment. These types of controls must be integrated in the IT solution implemented at the bank's branches. Some examples of internal controls in bank branch are given here:

- Work of one staff member is invariably supervised/ checked by another staff member, irrespective of the nature of work (Maker-Checker process).
- A system of job rotation among staff exists.
- Financial and administrative powers of each official/ position is fixed and communicated to all persons concerned.
- Branch managers must send periodic confirmation to their controlling authority on compliance of the laid down systems and procedures.
- All books are to be balanced periodically. Balancing is to be confirmed by an authorized official.
- Details of lost security forms are immediately advised to controlling so that they can exercise caution.
- Fraud prone items like currency, valuables, draft forms, term deposit receipts, traveler's cheques and other such security forms are in the custody of at least two officials of the branch.

(b) IT Controls in Banks

IT risks need to be mitigated by implementing the right type and level of controls in the automated environment. This is done by integrating controls into IT. Sample list of IT related controls are:

- The system maintains a record of all log-ins and log-outs.
- If the transaction is sought to be posted to a dormant (or inoperative) account, the processing is halted and can be proceeded with only with a supervisory password.

- The system checks whether the amount to be withdrawn is within the drawing power.
- The system flashes a message if the balance in a lien account would fall below the lien amount after the processing of the transaction.
- Access to the system is available only between stipulated hours and specified days only.
- Individual users can access only specified directories and files. Users should be given access only on a 'need-to-know basis' based on their role in the bank. This is applicable for internal users of the bank and customers.
- Exception situations such as limit excess, reactivating dormant accounts, etc. can be handled only with a valid supervisory level password.
- A user timeout is prescribed. This means that after a user logs-in and there is no activity for a pre-determined time, the user is automatically logged out of the system.
- Once the end-of-the-day process is over, the ledgers cannot be opened without a supervisory level password.

(c) Application Software - Configuration, Masters, Transactions and Reports

Application Software whether it is a high-end CBS software, ERP software or a simple accounting software, have primarily four gateways through which enterprise can control functioning, access and use the various menus and functions of the software. These are **Configuration**, **Masters**, **Transactions** and **Reports**.

The details of concepts of <u>Configuration</u>, <u>Masters</u>, <u>Transactions</u> have already been discussed in Chapter 1 in detail.

(i) Configuration: Some examples of configuration in the context of CBS software are given here:

- Defining access rules from various devices/terminals.
- Creation of User Types
- Creation of Customer Type, Deposit Type, year-end process
- User Access & privileges - Configuration & its management
- Password Management

(ii) Masters: Some examples of masters in context of CBS Software are as follows:

- **Customer Master:** Customer type, details, address, PAN details,
- **Employee Master:** Employee Name, Id, designation, level, joining details, salary, leave, etc.
- **Income Tax Master:** Tax rates applicable, Slabs, frequency of TDS, etc.

(iii) Transactions: Some examples of transactions in the context of CBS software are given here:

- **Deposit transactions:** opening of a/c, deposits, withdrawals, interest computation, etc.
- **Advances transactions:** opening of a/c, deposits, withdrawals, transfers, closure, etc.
- **ECS transactions:** Entry, upload, authorize/approve, update, etc.
- **General Ledger:** Expense accounting, interest computation update, charges update, etc.

(iv) Reports: Users at different levels use information in different form of reports - standard or adhoc reports, which are periodically generated or on demand. These reports could be used for monitoring the operations as also for tracking the performance or security. CBS software has extensive reporting features with standard reports and options to generate adhoc reports as required by user or the bank. Some examples of reports are as follows:

- Summary of transactions of day
- Daily General Ledger (GL) of day
- Activity Logging and reviewing
- MIS report for each product or service
- Reports covering performance/compliance;
- Reports of exceptions, etc.

The Table 5.3.2 provides illustrative list of Risks and their associated Controls in CBS.

Table 5.3.2: Sample listing of Risks and Controls w.r.t Application Controls

Risks	IT Controls
Interest may be incorrectly computed leading to incorrect recording of income/expenditure.	Interest is automatically correctly computed. Digits are rounded off appropriately. Interest is accurately accrued.
Inappropriate assignment of rate codes resulting in violation of business rules and/ or loss of revenue.	The interest rate code is defaulted at the account level and can be modified to a rate code carrying a higher or lower rate of interest only based on adequate approvals.
Absence of appropriate system validations may result in violation of business rules.	System validations have been implemented to restrict set up of duplicate customer master records.
Inappropriate reversal of charges resulting in loss of revenue.	System does not permit reversal of the charges in excess of the original amount charged.
Multiple liens in excess of the deposit value may result in inability to recover the outstanding in the event of a de-fault.	System prevents a single lien from exceeding the deposit value. It prevents marking of multiple liens against the same deposit, thus preventing the total liens exceeding the deposit account.
Inappropriate security or controls over system parameter settings resulting in unauthorized or incorrect changes to settings.	Access for changes made to the configuration, parameter settings is restricted to authorized user and require authorization/ verification from another user.
Failure to automate closure of NRE/ NRO accounts on change in residence status may result in regulatory non-compliance and undue benefits to customers.	On change of Customer status from NRI/ NRO to Resident on system, the system forces the closure of accounts opened for that customer under NRE/ NRO schemes, and to re-open the same under resident saving account schemes.

Inappropriate set up of accounts resulting in violation of business rules.	The system parameters are set up as per business process rules of the bank.
Failure to levy appropriate charges resulting in loss of revenue. Inappropriate levy of charges, resulting in customer disputes.	System does not permit closing of an account having zero balance without re- covering the applicable account closure charges.
Inappropriate security or controls over file upload transactions resulting in intentional or inadvertent accounting errors.	Automated file upload process to the NPA Provisioning System, exist eliminating the need for manual intervention.
Incorrect classification and provisioning of NPAs, resulting in financial misstatement.	Configuration/customization exists in the application to perform the NPA classification as per relevant RBI guidelines.
Failure to levy appropriate charges resulting in loss of revenue. Inappropriate levy of charges, resulting in customer disputes.	The charges applicable for various transactions as per account types are properly configured as per bank rules. The Charges are as in compliances with RBI and bank's policies.
Duplicate asset records may be created. Ownership of asset may not be clearly established.	Unique Id is created for each asset. Each asset is assigned to specific business unit and user to establish owner- ship.

(d) CBS: Core Business Processes - Relevant Risks and Controls

Banks carry out variety of functions across the broad spectrum of products offered by them. Some of the key products that are provided by most commercial banks are Current and Savings Accounts (CASA), Credit Cards, Loans and Advances, Treasury and Mortgages.

Below is a high-level overview (illustrative and not exhaustive) of some of these processes with its relevant flow and indicative key risks and controls across those processes. The flow and process as well as relevant risk and control may differ from bank to bank however below information should give a basic idea to students about these processes where CBS and other relevant applications are used and what specific risk and controls might be relevant in such cases.

I. Business process flow of Current & Savings Accounts (CASA)

(a) Process Flow of CASA facility (as shown in the Fig. 5.3.1)

(i) Either the customer approaches the relationship manager to apply for a CASA facility or will apply the same through internet banking, the charges/ rates for the facility are provided by the relationship manager on basis of the request made by the customer.

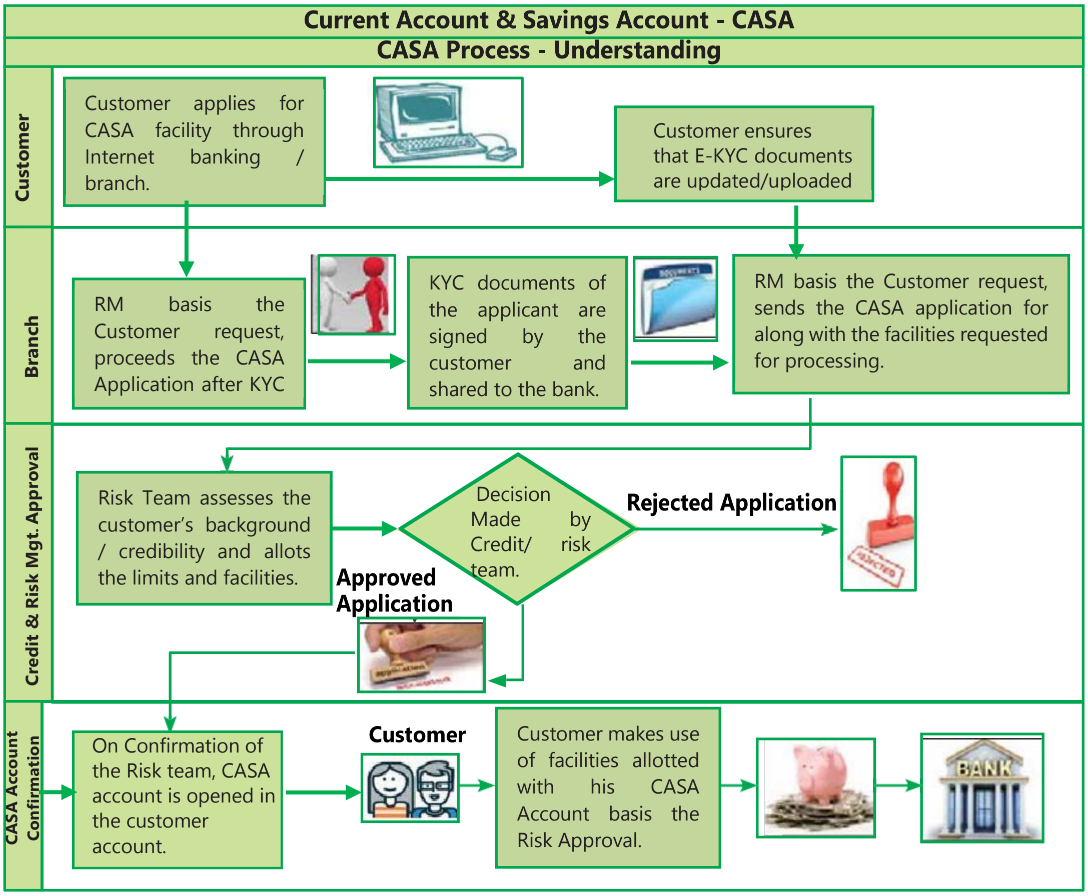

Current Account & Savings Account - CASA
CASA Process - Understanding
Customer
Customer applies for CASA facility through Internet banking / branch.
Customer ensures that E-KYC documents are updated/uploaded
Branch
RM basis the Customer request, proceeds the CASA Application after KYC
KYC documents of the applicant are signed by the customer and shared to the bank.
RM basis the Customer request, sends the CASA application for along with the facilities requested for processing.
Credit & Risk Mgt. Approval
Risk Team assesses the customer's background / credibility and allots the limits and facilities.
Decision Made by Credit/ risk team.
Rejected Application
Approved Application
CASA Account Confirmation
On Confirmation of the Risk team, CASA account is opened in the customer account.
Customer
Customer makes use of facilities allotted with his CASA Account basis the Risk Approval.
BANK

Fig. 5.3.1: CASA Process

(ii) Once the potential customer agrees for availing the facilities/products of the bank, the relationship manager request for the relevant documents i.e. KYC and other relevant documents of the customer depending upon the facility/product. KYC (Know Your Customer) is a process by which banks obtain information about the identity and address of the customers. KYC documents can be Passport, Driving License, etc.

(iii) The documents received from the customers are handed over to the Credit team / Risk team for sanctioning of the facilities/limits of the customers.

(iv) Credit team verifies the document's, assess the financial and credit worthiness of the borrowers and updates facilities in the customer account.

(v) Current / Account savings account along with the facilities requested are provided to the customer for daily functioning.

(vi) Customers can avail facilities such as cheque deposits / withdrawal, Cash deposit / withdrawal, Real Time Gross Settlement (RTGS), National Electronics Funds Transfer System (NEFT), Electronic Clearing Service (ECS), Overdraft Fund Transfer services provided by the bank.

(b) Risk & Controls around the CASA Process (discussed in the Table 5.3.3)

Table 5.3.3: Risk & Controls around the CASA Process

S.No.	Risk	Key Controls
1.	Credit Line setup is unauthorized and not in line with the bank's policy.	The credit committee checks that the Financial Ratios, the Net-worth, the Risk factors and its corresponding mitigating factors, the Credit Line offered and the Credit amount etc. is in line with Credit Risk Policy and that the Client can be given the Credit Line.
2.	Credit Line setup in CBS is unauthorized and not in line with the bank's policy.	Access rights to authorize the credit limit in case of account setup system should be restricted to authorized personnel.
3.	Customer Master defined in CBS is not in accordance with the Pre-Disbursement Certificate.	Access rights to authorize the customer master in CBS should be restricted to authorized personnel.
4.	Inaccurate interest / charge being calculated in CBS.	Interest on fund based facilities is automatically calculated in the CBS as per the defined rules.
5.	Unauthorized personnel approving the CASAS transaction in CBS.	Segregation of Duties to be maintained between the initiator and authorizer of the transaction for processing transaction in CBS.

6.	Inaccurate accounting entries generated in CBS.	Accounting entries are generated by CBS basis the facilities requested by the customer and basis defined configurations for those facilities in CBS.

II. Business Process flow of Credit Cards

(a) Process Flow of Issuance of Credit Card Facility (as shown in the Fig. 5.3.2)

(i) Either the customer approaches the relationship manager to apply for a credit card facility or customer will apply the same through internet banking, the charges/rates for the facility are provided by the relationship manager basis the credit application made by the customer.

(ii) Once the potential customer agrees for availing the facilities/products of the bank, the relationship manager request for the relevant documents i.e. KYC and other relevant documents of the customer depending upon the facility/product.

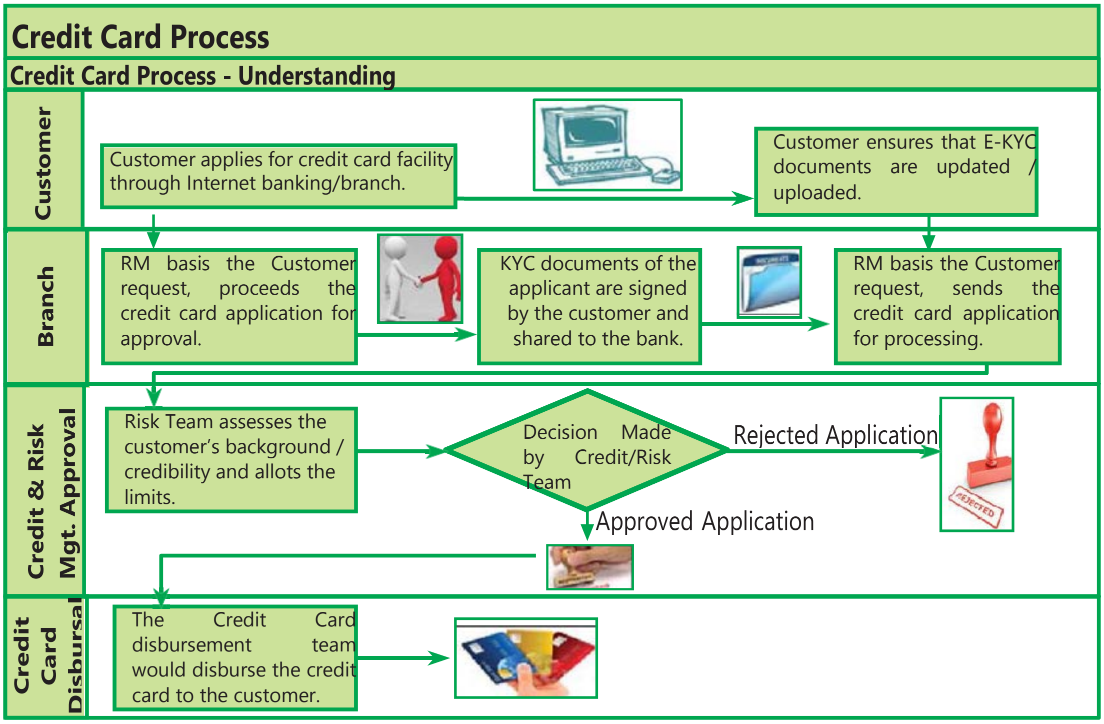

Credit Card Process
Credit Card Process - Understanding
Customer
Customer applies for credit card facility through Internet banking/branch.
Customer ensures that E-KYC documents are updated / uploaded.
Branch
RM basis the Customer request, proceeds the credit card application for approval.
KYC documents of the applicant are signed by the customer and shared to the bank.
RM basis the Customer request, sends the credit card application for processing.
Credit & Risk Mgt. Approval
Risk Team assesses the customer's background / credibility and allots the limits.
Decision Made by Credit/Risk Team
Rejected Application
REJECTED
Approved Application
Credit Card Disbursal
The Credit Card disbursement team would disburse the credit card to the customer.

Fig. 5.3.2: Process Flow of Issuance of Credit Card Facility

(iii) The documents received from the customers are handed over to the Credit team for sanctioning of the facilities/limits of the customers.

(iv) Credit team verifies the document's, assesses the financial and credit worthiness of the borrowers and issues a credit limit to the customer in CBS and allots a credit card.

(v) Credit Card is physically transferred to the customer's address.

(b) Process Flow of Sale - Authorization process of Credit Card Facility (as shown in the Fig. 5.3.3)

(i) Customer will swipe the credit card for the purchase made by him/her on the POS machine (Point of Sale) at merchant's shop/establishment.

(ii) POS (Point of Sale) will process the transaction only once the same is authenticated.

(iii) The POS (Point of Sale) will send the authentication request to the merchant's bank (also referred as 'acquiring bank') which will then send the transaction authentication verification details to the credit card network (such as VISA, MASTER CARD, AMEX, RUPAY) from which the data will be validated by the credit card issuing bank within a fraction of seconds.

(iv) Once the transaction is validated, the approval message is received from credit card issuing bank to the credit card network which then flows to the merchant's bank and approves the transaction in the POS (Point of Sale) machine.

(v) The receipt of the transaction is generated and the sale is completed. The transaction made is charged during the billing cycle of that month.

(c) Process Flow of Clearing & Settlement process of Credit Card Facility (as shown in the Fig. 5.3.3)

(i) The transaction data from the merchant is transferred to the merchant's bank. Merchant's bank clears settlement amount to Merchant after deducting Merchant fees. Merchant's bank, in turn now provides the list of settlement transactions to the credit card network which then provides the list of transactions made by the customer to the credit card issuing bank.

(ii) The credit card issuing bank basis the transactions made, clears the amount to Merchant's bank but after deducting interchange transaction fees.

(iii) At the end of billing cycle, card issuing company charges the customer's credit card account with those transactions in CBS.

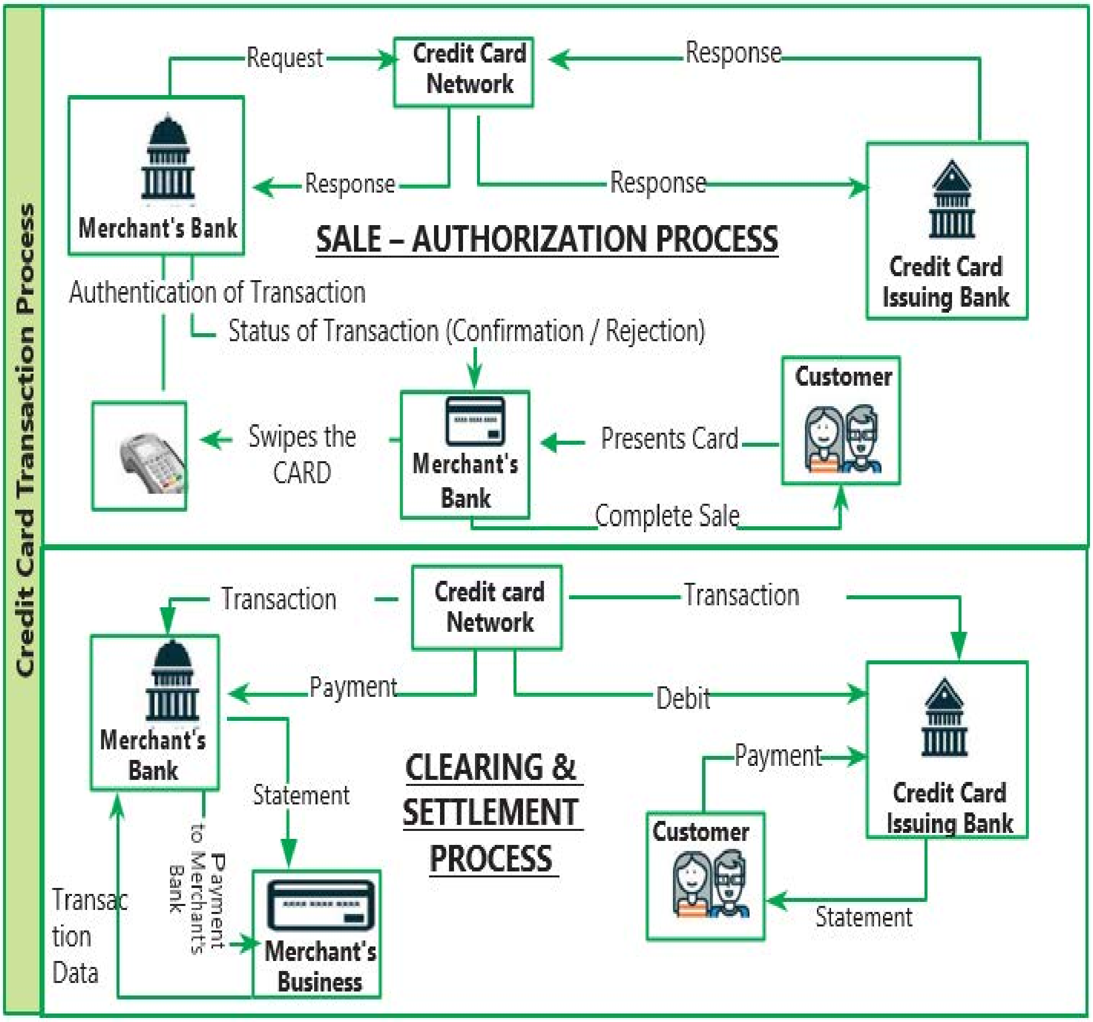


Fig. 5.3.3: Process Flow of Sale - Authorization and Clearing & Settlement of Credit Card Facility

(d) Risks and Controls around the Credit Card Process (Refer Table 5.3.4)

Table 5.3.4: Risks and Controls around the Credit Card Process

S. No.	Risks	Key Controls
1.	Credit Line setup is unauthorized and not in line with the bank's policy	The credit committee checks that the Financial Ratios, the Net-worth, the Risk factors and its corresponding mitigating factors, the Credit Line offered and the Credit amount etc. is in line with Credit Risk Policy and that the Client can be given the Credit Line.
2.	Credit Line setup is unauthorized and not in line with the bank's policy.	Access rights to authorize the credit limit in the credit card system should be restricted to authorized personnel.
3.	Masters defined for the customer are not in accordance with the Pre-Disbursement Certificate.	Access rights to authorize the customer master in credit card system should be restricted to authorized personnel, Segregation of duties exist in credit card system such that the system restricts the maker having checker rights to approve the facilities booked by self in the credit card system.
4.	Credit Line setup can be breached.	Transaction cannot be made if the aggregate limit of out- standing amount exceeds the credit limit assigned to customer.
5.	Inaccurate interest / charge being calculated in the Credit Card system.	Interest on fund based credit cards and charges are automatically calculated in the credit card system as per the defined masters.
6.	Inaccurate reconciliations performed.	Daily reconciliation for the balances received from credit card network with the transactions updated in the credit card system on card network level.

III. Business Process Flow of Mortgages

A **Mortgage loan** is a secured loan which is secured on the borrower's property by marking a lien on the property as collateral for the loan. If the borrower stops paying, then the lender has the first charge on the property. Mortgages are used by individuals and businesses to make large real estate purchases without paying the entire value of the purchase up front. Over the period of many years, the borrowers repay the loan amount along with interest until there is no outstanding.

(a) Types of Mortgage Loan

- **Home Loan:** This is a traditional mortgage where customer has an option of selecting fixed or variable rate of interest and is provided for the purchase of property
- **Top Up Loan:** Here the customer already has an existing loan and is applying for additional amount either for refurbishment or renovation of the house
- **Loans for Under Construction Property**: In case of under construction properties the loan is disbursed in tranches / parts as per construction plan.

(b) Process Description (as shown in the Fig. 5.3.4)

(i) Loans are provided by the lender which is a financial institution such as a bank or a mortgage company. There are two types of loan widely offered to customer first is fixed rate mortgage where rate of interest remains constant for the life of the loan second is variable/floating rate mortgage where rate of interest is fixed for a period but then it fluctuates with the market interest rates.

(ii) Borrower / Customer approach the bank for a mortgage and relationship manager/ loan officer explains the customer about home loan and its various feature. Customer to ill loan application and provide requisite KYC documents (Proof of Identity, Address, Income and obligation details etc.) to the loan officer.

(iii) Loan officer reviews the loan application and sends it to Credit risk team who will calculate the financial obligation income ratio which is to determine customer's financial eligibility on how much loan can be provided to the customer. This is done basis the credit score as per Credit Information Bureau (India) Limited (CIBIL) rating, income and expense details and Rate of Interest at which loan is offered. Once financial eligibility is determined, then along with customer documents the details are sent to the underwriting team for approval.

(iv) Underwriting team will verify the financial (applicant's credit history) and employment information of the customer. Underwriter will ensure that the loan provided is within the lending guidelines and at this stage provide conditional approval along with the list of documents required.

(v) As per the property selected by the customer, loan officer will provide the property details along with requisite documents (property papers etc.) to the legal and valuation team. Legal team will carry out title search on the property which is to determine legal owner of the property, any restrictions or any lien on the property etc. Valuation team will carry out valuation of property and determine its value.

(vi) Further verification of property to determine whether property is built as per the approved plan, whether builder has received requisite certificates, age of building to determine whether it will withstand the loan tenure, construction quality.

(vii) Legal and valuation team will send their report to the operations team which will generate letter of offer / Offer letter to customer which entails all details of loan such as loan amount, rate of interest, tenor, monthly installment, security address, fee/charges details and term and conditions.

(viii) Customer will agree to loan agreement which is offered by signing the offer letter. Loan officer will notarize all the loan documents and are send back to lender operations team.

(ix) Once signed offer letter is received the operations team will release or disburse fund and prepare a cashier order. Cashier order is provided to customer in exchange of mandatory original property documents. Once exchange is carried out successfully, banks place a charge or lien on the property so that incase of default the first charge is with the bank to recover the money.

(ix) Post disbursement of loan customer can carry out various loan servicing activity by visiting the branch or via online mode amendments such as interest rate change, change in monthly installment, prepayment of loan amount and foreclosure of loan etc.

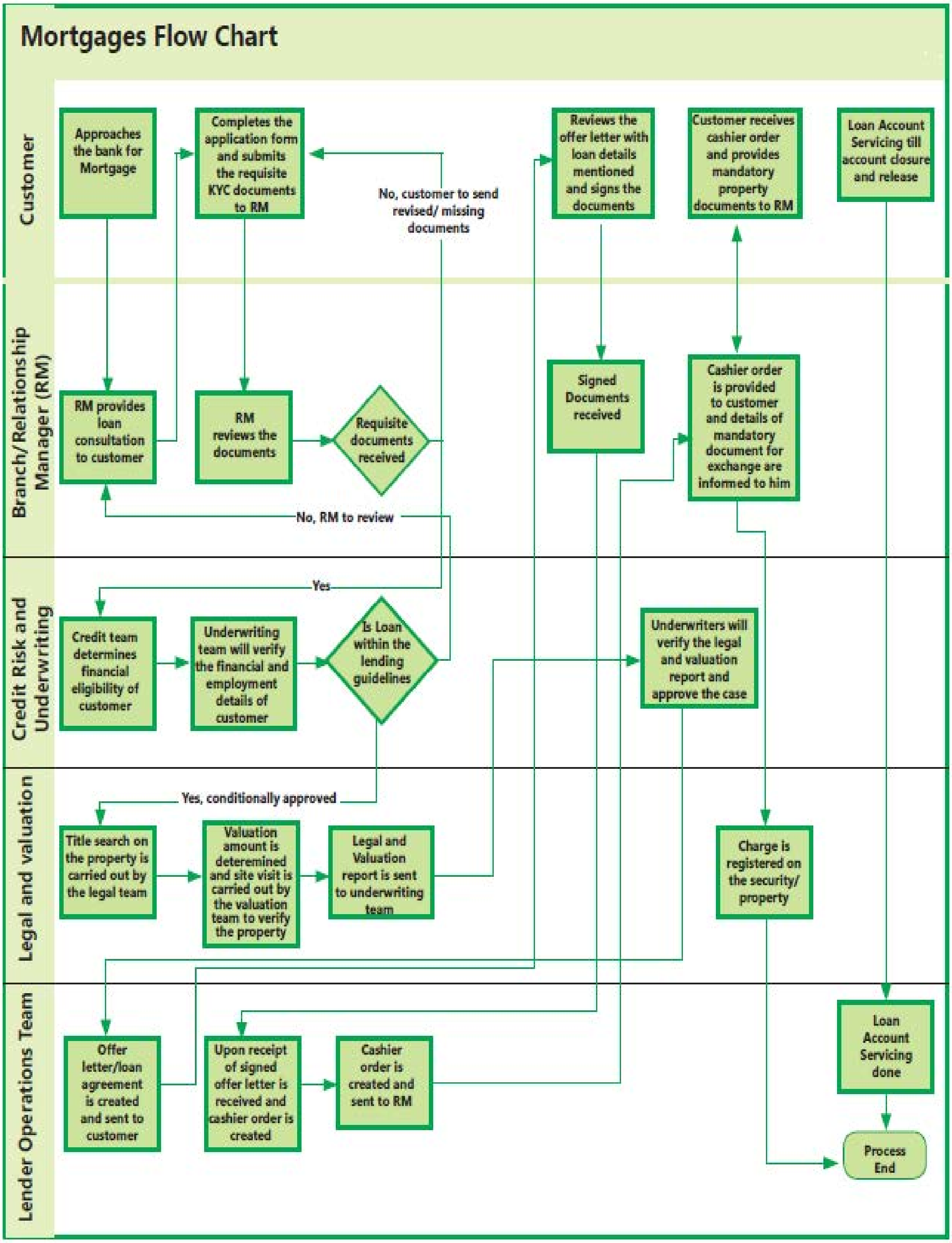

Mortgages Flow Chart
Customer
Branch/Relationship Manager (RM)
Credit Risk and Underwriting
Legal and valuation
Lender Operations Team
Approaches the bank for Mortgage
Completes the application form and submits the requisite KYC documents to RM
No, customer to send revised/ missing documents
Reviews the offer letter with loan details mentioned and signs the documents
Customer receives cashier order and provides mandatory property documents to RM
Loan Account Servicing till account closure and release
RM provides loan consultation to customer
RM reviews the documents
Requisite documents received
Signed Documents received
Cashier order is provided to customer and details of mandatory document for exchange are informed to him
No, RM to review
Yes
Credit team determines financial eligibility of customer
Underwriting team will verify the financial and employment details of customer
Is Loan within the lending guidelines
Underwriters will verify the legal and valuation report and approve the case
Yes, conditionally approved
Title search on the property is carried out by the legal team
Valuation amount is deteremined and site visit is carried out by the valuation team to verify the property
Legal and Valuation report is sent to underwriting team
Charge is registered on the security/ property
Offer letter/loan agreement is created and sent to customer
Upon receipt of signed offer letter is received and cashier order is created
Cashier order is created and sent to RM
Loan Account Servicing done
Process End

Fig. 5.3.4: Business process flow of Mortgages

(c) Risk & Controls around the Mortgage Process (discussed in the Table 5.3.5)

Table 5.3.5: Risk & Controls around the Mortgage Process

S. No.	Risk	Key Controls
1.	Incorrect customer and loan details are captured which will affect the over- all downstream process.	There is secondary review performed by an independent team member who will verify loan details captured in core banking application with offer letter.
2.	Incorrect loan amount disbursed.	There is secondary review performed by an independent team member who will verify loan amount to be disbursed with the core banking application to the signed offer letter.
3.	Interest amount is incorrectly calculated and charged.	Interest amount is auto calculated by the core banking application basis loan amount, ROI and tenure.
4.	Unauthorized changes made to loan master data or customer data.	System enforced segregation of duties exist in the core banking application where the person putting in of the transaction cannot approve its own transaction and reviewer cannot edit any details submitted by person putting data.

IV. Business Flow of Treasury Process

Investments Category are Government Securities (Gsec), shares, other investments, such as, Commercial Papers, Certificate of Deposits, Security Receipts, (ass Through Certificates, Units of Mutual Funds, Venture Capital Funds and Real Estate Funds Debentures and Bonds.

Products in Trading category are Forex and Derivatives (Over-The-Counter (OTC) and Exchange traded) the products involved are Options, Swaps, Futures, Foreign Exchange (FX) forwards, Interest derivatives).

(a) **Core areas of Treasury Operations:** The core areas of treasury operations in a bank can be functionally divided into the following broad compartments as mentioned below:

- Dealing Room Operations (Front office operations);
- Middle Office (Market Risk department / Product Control Group); and
- Backoffice.

(i) **Front Office:** The **Front Office** operations consist of dealing room operations wherein the dealers enter into deal with the various corporate and interbank Counter-parties. Deals are entered by dealers on various trading /Communication platform such as Reuters' system, telephonic conversation, Brokers or any other private channel with the respective counter-party. The dealers are primarily responsible to check for counter-party credit Limits, eligibility, and other requirements of the Bank before entering into the deal with the customers. Dealers must ensure that all risk/credit limits are available before entering into a deal. Also, the deal must not contravene the current regulations regarding dealing in INR with overseas banks/counter-parties. All counter-parties are required to have executed the International Swaps and Derivatives Association ('ISDA') agreement as well as pass a board resolution allowing it to enter into derivatives contract. As soon as the deal is struck with counter-party, the deal details are either noted in a manual deal pad or punched in front office system of the Bank which gets queued in for authorization.

(ii) **Middle Office: Middle Office** includes risk management, responsibility for treasury accounting, and documentation of various types, producing the financial results, analysis and budget forecasts for the treasury business unit, input into regulatory reporting. Risk management can range from agreeing overnight cash positions for the trading room through to full-risk modeling associated with derivatives trading and hedging. It is also responsible for monitoring of counter- party, country, dealer and market-related limits that have been set and approved in other areas of the bank such as the credit department.

(iii) Back Office Operations: The mainstream role of the **Back Office** is in direct support of the trading room or front office. This includes verification by confirmation, settlement, checking existence of a valid and enforceable International Swap Dealers Association ('ISDA’) agreement and reconciliation of nostro accounts (a bank account held by a UK bank with a foreign bank, usually in the currency of that country) as soon as possible. An important development in the back office has been the advent of Straight-Through Processing (STP), also called 'hands-off’ or exception processing. This has been made possible through enhancement of system to real time on line input in the trading room, which in turn has meant that the back office can recall deals input in the trading room to verify from an eternal source. Back office is also involved in a number of reconciliation processes, including the agreement of traders’ overnight positions, Nostro accounts and brokerage. The critical one is FOBO (Front Office/ Back Office) reconciliation to ensure the completeness and accuracy of trades/ deals done for the day.

In practice, this is done automatically, comparing incoming data from brokers and counter-parties and investigating exceptions. With the introduction of full trading systems, the deal is 'confirmed’ as it is done, allowing the back office to concentrate principally on exception reporting, settlement and risk control. One of the basic tenets for a treasury area in a bank is the strict segregation of duties and location between the front and back office, the latter controlling confirmations and settlement transactions.

(b) Process flow for Bank Treasury Operations: Process flow for Bank Treasury Operations is provided in the Fig. 5.3.6.

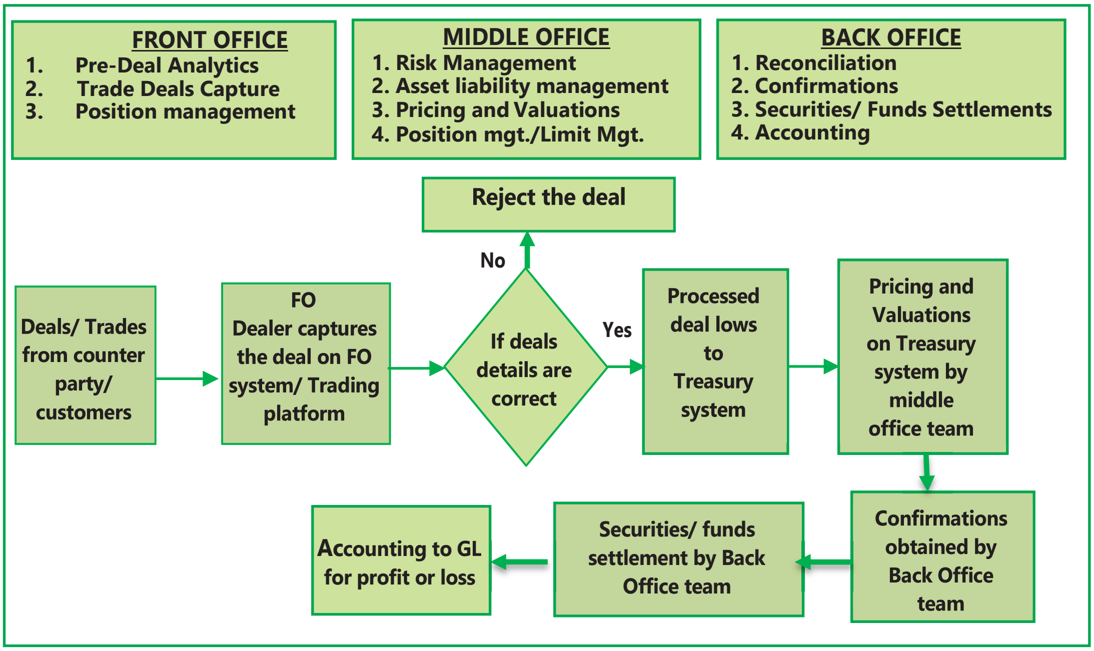

FRONT OFFICE
1. Pre-Deal Analytics
2. Trade Deals Capture
3. Position management
MIDDLE OFFICE
1. Risk Management
2. Asset liability management
3. Pricing and Valuations
4. Position mgt./Limit Mgt.
BACK OFFICE
1. Reconciliation
2. Confirmations
3. Securities/ Funds Settlements
4. Accounting
Reject the deal
No
Yes
Deals/ Trades from counter party/ customers
FO Dealer captures the deal on FO system/ Trading platform
If deals details are correct
Processed deal lows to Treasury system
Pricing and Valuations on Treasury system by middle office team
Confirmations obtained by Back Office team
Securities/ funds settlement by Back Office team
Accounting to GL for profit or loss

Fig. 5.3.6: Process Flow for Bank Treasury Operations

(c) Risk & Controls around the Treasury Process: (Listed in the Table 5.3.6)

Table 5.3.6: Risk & Controls around the Treasury Process

S. No	Risk	Key Controls
1.	Unauthorized securities setup in systems such as Front office/Back office.	Appropriate Segregation of duties and review controls around securities master setup/ amendments.
2.	Inaccurate trade is processed.	Appropriate Segregation of duties and review controls to ensure the accuracy and authorization of trades.
3.	Unauthorized confirmations are processed.	Complete and accurate confirmations to be obtained from counter-party.
4.	Insufficient Securities available for Settlement	Effective controls on securities and margins.

5.	Incomplete and inaccurate data flow between systems.	Inter-system reconciliations, Interfaces and batch processing controls.
6.	Insufficient funds are available for settlements.	Controls at CCIL/NEFT/RTGS settlements to ensure the margin funds availability and the timely funds settlements.
7.	Incorrect Nostro payments processed.	Controls at Nostro reconciliation and payments.

V. Loans and Trade Finance Process

The business of lending, which is main business of the banks, carry certain inherent risks and bank cannot take more than calculated risk whenever it wants to lend. Hence, lending activity has to necessarily adhere to certain principles. The business of lending is carried on by banks offering various credit facilities to its customers. Basically, various credit facilities offered by banks are generally repayable on demand. A bank should ensure proper recovery of funds lent by it and acquaint itself with the nature of legal remedies available to it and also law affecting the credit facilities provided by it.

(a) **Classification of Credit Facilities:** These may broadly be classified as under:

(i) **Fund Based Credit Facilities:** Fund based credit facilities involve outflow of funds meaning thereby the money of the banker is lent to the customer. They can be generally of following types:

- Cash Credits/Overdrafts
- Demand Loans/Term loans
- Bill Discounting

(ii) **Non-Fund Based Credit Facilities:** In this type of credit facility, the banks funds are not lent to the customer and they include Bank Guarantees and Letter of Credit.

Overall the process flow in either of the above facilities remains the same. Below narratives provide a very high-level summary of these processes.

(I) Customer Master Creation in Loan Disbursement System (which may be your CBS or may be a separate system which periodically interfaces with CBS)

(i) The relationship manager across locations identifies the potential customers and approaches them with the details of the products/facilities and the charges/rates or the customer may directly approach the bank for availing the facilities.

(ii) Once the potential customer agrees for availing the facilities/products of the bank, the relationship manager request for the relevant documents i.e. KYC and other relevant documents of the customer depending upon the facility/product.

(iii) The documents received from the customers are handed over to the Credit team of bank for sanctioning of the facilities/limits of the customers.

(iv) Credit team verifies the document's, assesses the financial and credit worthiness of the borrowers and issues a sanction letter to the customer.

(v) Sanction letter details the terms of the facilities and the credit limits the customer is eligible e.g. how much loan can be offered to the customer.

(vi) Once the customer agrees with the terms of the sanction letter, the credit team prepares a Pre-Disbursement Certificate (PDC) containing the details of all the facilities & limits approved for the customer and send it to the disbursement team i.e. the team who is responsible for disbursing the loan amount to customer.

(vii) The disbursement team verifies the PDC and creates customer account and master in the Loan Disbursement System. The disbursement team member also assigns the limits for various products as per PDC.

(viii) Once the limits are assigned to the customer, the customer can avail any of the facilities/products up to the assigned credit limits.

(II) Loan Disbursal / Facility Utilization and Income Accounting

(i) Customer may approach the bank for availing the product/facility as per the sanction letter.

(ii) The facility/product requested are offered to the customer after verifying the customer limits in the Loan Disbursal System which normally would be CBS or may be a separate system which later interfaces with CBS on periodic basis.

(iii) In case of the fund based loan - Term Loan /Overdraft/Cash credits, the funds are disbursed to the customer's bank accounts and the corresponding asset is recorded in a loan account recoverable from the customer. Interest is generally accrued on a daily basis along with the principal as per the agreed terms are recovered from the customer.

(iv) In case of bills discounting product, the customer is credited the invoice amount excluding the interest amount as per the agreed rates. Interest income is generally accrued on a daily basis. Receivable is booked in a loan account.

(v) In case of non- fund based facilities, the facilities are granted to the customer up to the assigned limits in the loan disbursement system. Contingent entries are posted for asset and liabilities. Commission is normally charged to the customer account upfront on availing the facility and is accrued over the tenure of the facilities granted to the customer.

Table 5.3.7: Risk & Controls around the Treasury Process

Sr. No.	Product	Income for banks	Accounting of Income
1.	Cash Credit/ Overdraft	Interest on Cash Credits/ Overdraft balances.	Interest accrued on a daily basis at the agreed rates.
2.	Demand draft/ Term Loan's	Interest on Demand draft/Term loan.	Interest accrued on a daily basis at the agreed rates.
3.	Bill Discounting	Discounting Income.	Interest accrued on a daily basis at the agreed rates.
4.	Bank Guarantee	Commission.	Commission accrued over the tenure of the bank guarantee.
5.	Letter of Credit	Commission Income.	Commission accrued over the tenure of the bank guarantee.

(b) Process flow for Fund based loans (Fig. 5.3.6)

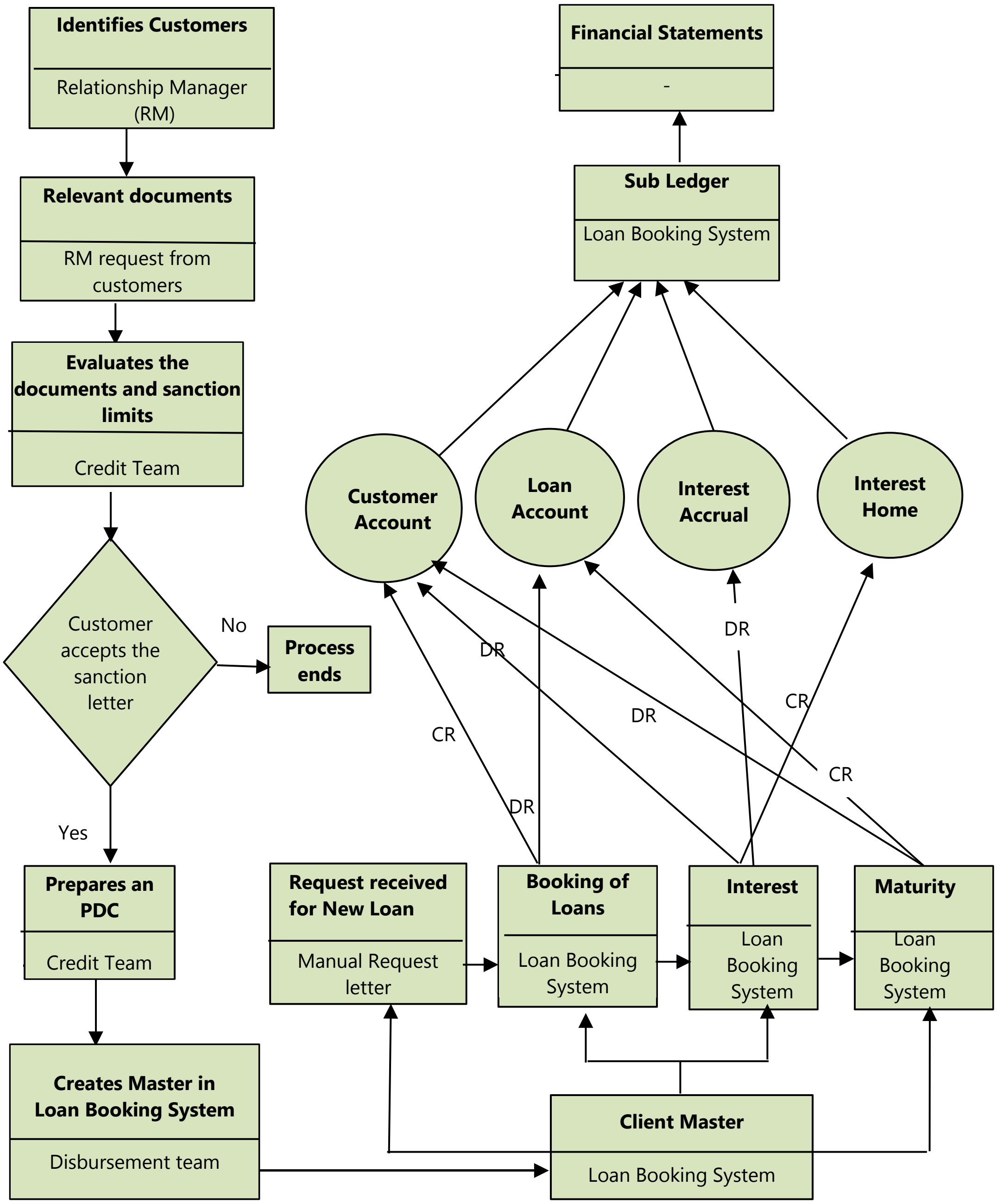


Fig. 5.3.6: Process Flow for Fund based Loans

(c) Process flow for Non-fund based loans (Fig. 5.3.7)

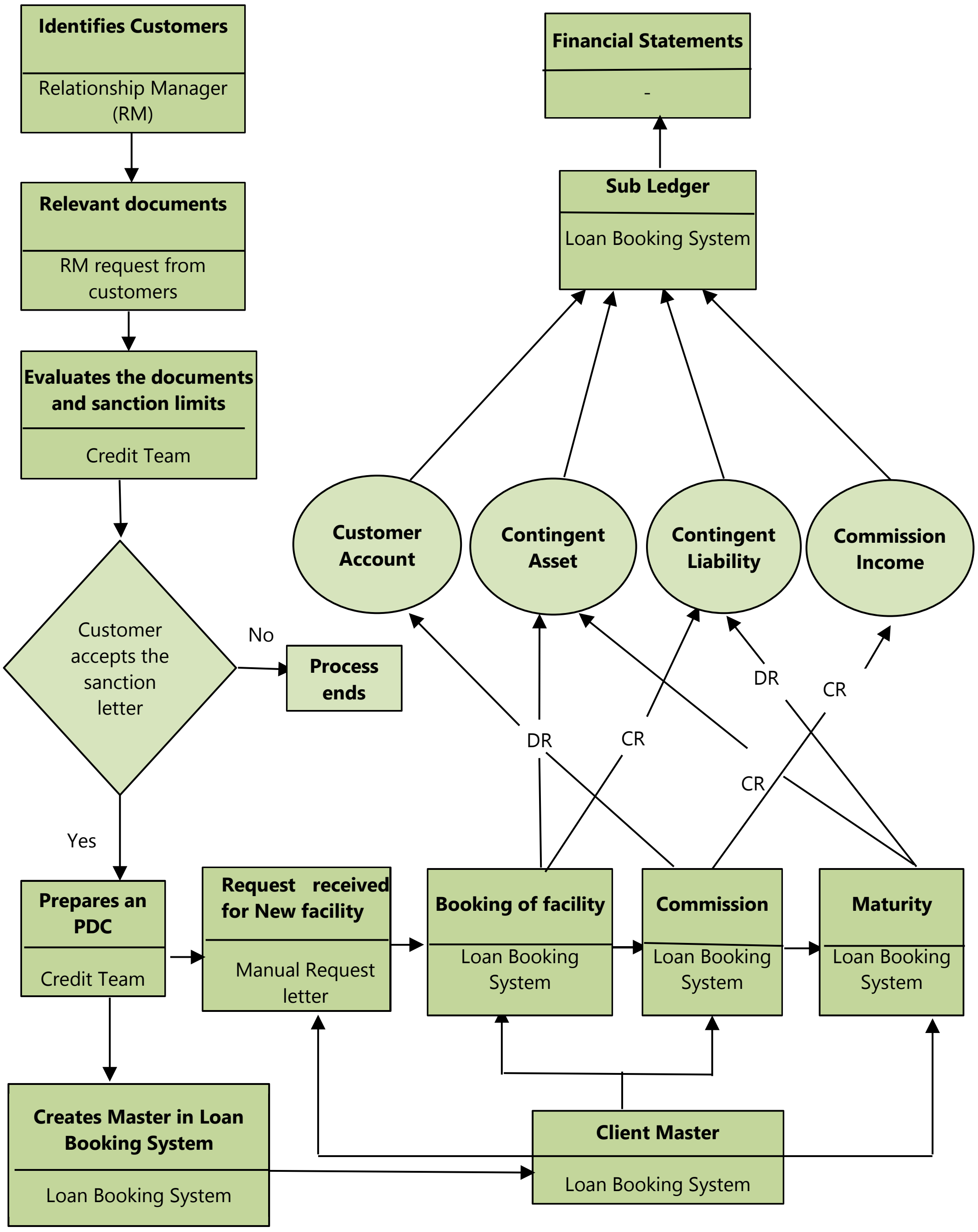


Fig. 5.3.7: Process Flow for Non - Fund based Loans

(d) **Risk and Controls in the Loans and Advances Process:** These are provided in the Table 5.3.8.

Table 5.3.8: Risk & Controls in the Loans and Advances Process

S. No.	Risk	Key Controls
1.	Credit Line setup is unauthorized and not in line with the bank's policy.	The credit committee checks that the Financial Ratios, the Net-worth, the Risk factors and its corresponding mitigating factors, the Credit Line offered and the Credit amount etc. is in line with Credit Risk Policy and that the Client can be given the Credit Line.
2.	Credit Line setup is unauthorized and not in line with the bank's policy.	Access rights to authorize the credit limit in Loan Booking system/CBS should be restricted to authorized personnel.
3.	Masters defined for the customer are not in accordance with the (re Disbursement Certificate.	Access rights to authorize the customer master in Loan Booking system/CBS should be restricted to authorized personnel. Segregation of duties exists in Loan Disbursement system. The system restricts the maker having checker rights to approve the loan/facilities booked by self in loan disbursal system
4.	Credit Line setup can be breached in Loan disbursement system/CBS.	Loan disbursement system/CBS restricts booking of loans/ facilities if the limit assigned to the customer is breached in Loan disbursement system/CBS.
5.	Lower rate of interest/ Commission may be charged to customer.	Loan disbursement system/CBS restricts booking of loans/ facilities if the rate charged to the customer are not as per defined masters in system.
6.	Facilities/Loan's granted may be unauthorized/in-appropriate	Segregation of duties exists in Loan Disbursement system. The system restricts the maker having checker rights to approve the loan/facilities booked by self in loan disbursal system
7.	Inaccurate interest / charge being calculated in the Loan disbursal system	Interest on fund based loans and charges for non-fund based loans are automatically calculated in the Loan disbursal system as per the defined masters.

5.4 REPORTING SYSTEMS AND MIS, DATA ANALYTICS AND BUSINESS INTELLIGENCE

The fundamental concepts of these topics are elaborately provided in the earlier 'Chapter 2 Financial and Accounting Systems' of the study material.

Risk Prediction for Basel III, based on Artificial Intelligence

Basel III is a comprehensive set of reform measures, developed by the Basel Committee on Banking Supervision, to strengthen the regulation, supervision and risk management of the banking sector. These measures aim to improve the banking sector's ability to absorb shocks arising from financial and economic stress, whatever the source and to improve risk management and governance. One of the dimensions of Basel III is determining capital adequacy based on risk assessment.

One of the critical areas of risk assessment is based on assessment of available data. It is hence important to refresh our understanding of the concept of a Data Warehouse. Data from CBS database is transferred to a Data Warehouse. Data Warehouse stores data in multi-dimensional cubes (unlike the rows and columns structures of tables in a traditional database of CBS). Data in the Data Warehouse is generally never purged. So, there is huge data accumulated over years.

For measurement and assessment of banking risks, we need to bear in mind that many complex business relationships and risks cannot be quantified statistically through linear models of risk assessment. Hence, the traditional MIS Reports and Decision-making Systems do not address answers to random questions on the data.

The only comprehensive and accurate solution for this problem is using artificial neural network logic (Artificial Intelligence), wherein algorithms based on neural networks are executed on the data the Data Warehouse, so as to understand hidden trends, which in turn helps in risk assessment.

This improves the management of banking risks and banking risk prediction, and in- turn, the assessment of capital adequacy under Basel III.

5.5 APPLICABLE REGULATORY AND COMPLIANCE REQUIREMENTS

5.5.1 Impact of Technology in Banking

The following Fig. 5.5.1 shows the four key components of banking business with controls pervading all the four areas of business process, policies and procedures, regulatory requirements and organization structure. However, in the CBS environment, technology is the encompasses all the four critical components which are business processes, policies and procedures, regulatory requirements and organization structure. All control relevant for all four components are embedded inside and facilitated through technology. The same technology platform is configured as per specific business style of the bank to provide new products and services. The dependence on technology in a bank is also very high. If IT fails, then none of the business processes can be performed. Hence, it is important to understand how the four components of banking business are configured, maintained and updated using technology. As per policy directives of regulators, the banking software should be configured or updated. The controls also need to be implemented and updated at different layers of technology such as system software, network, database, application software, etc.

Earlier, technology was a tool and used in specific department of the bank but now with CBS, Technology has become all-pervasive and has become integral for doing banking. Further, all the business and control aspects of the bank as a whole such as banking business processes, policies and procedures of the bank, regulatory and compliance requirements applicable to the bank and the organization structure of the bank are in-built into the technology through configuration, setting of parameters and controls at different layers of technology.

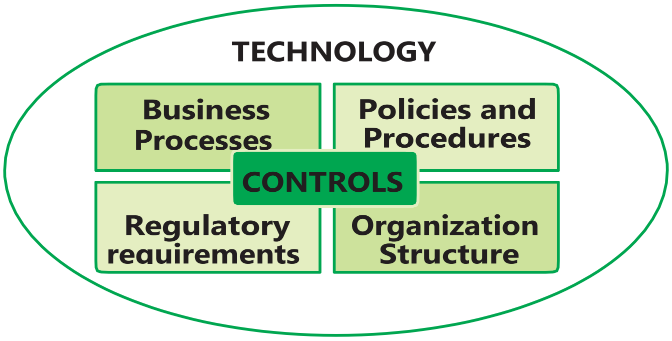


Fig. 5.5.1: Technology and Business Process Components

5.5.2 Money Laundering

Money Laundering is the process by which the proceeds of the crime and the true ownership of those proceeds are concealed or made opaque so that the proceeds appear to come from a legitimate source. The objective in money laundering is to conceal the existence, illegal source, or illegal application of income to make it appear legitimate. Money laundering is commonly used by criminals to make 'dirty' money appear 'clean' or the profits of criminal activities are made to appear legitimate.

I. Stages of Money Laundering (Refer Fig. 5.5.2)

1. Placement

The first stage involves the **Placement** of proceeds derived from illegal activities - the movement of proceeds, frequently currency, from the scene of the crime to a place, or into a form, less suspicious and more convenient for the criminal.

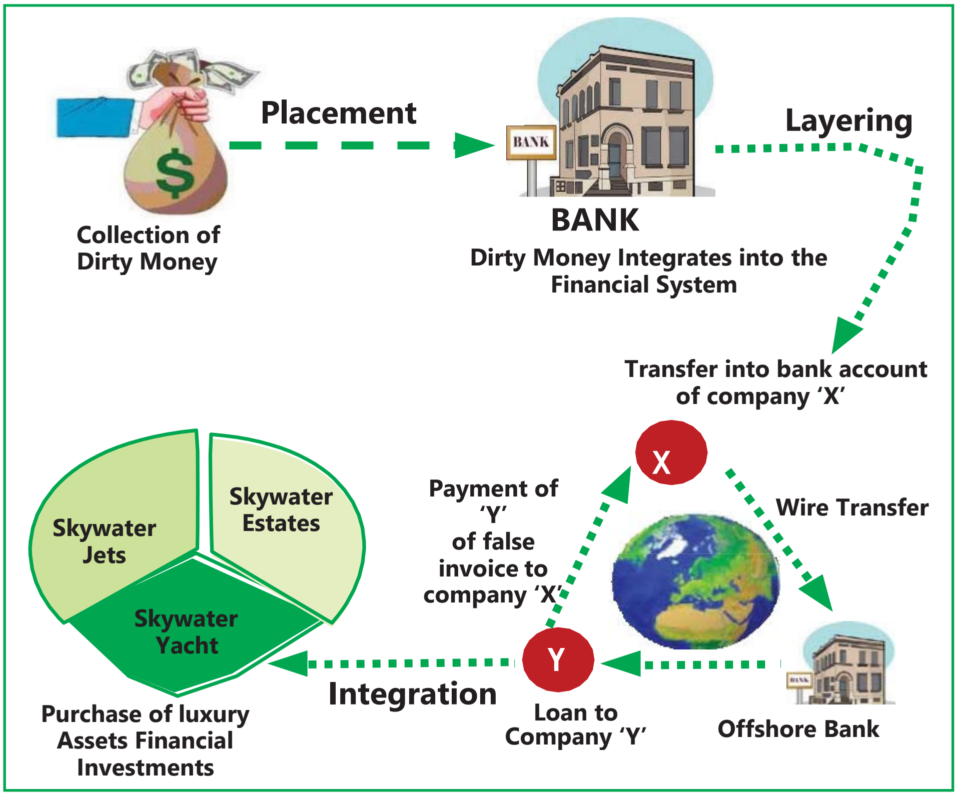

Placement
Collection of Dirty Money
BANK
BANK
Dirty Money Integrates into the Financial System
Layering
Transfer into bank account of company 'X'
X
Wire Transfer
Offshore Bank
Y
Loan to Company 'Y'
Payment of 'Y' of false invoice to company 'X'
Integration
Skywater Jets
Skywater Estates
Skywater Yacht
Purchase of luxury Assets Financial Investments

Fig. 5.5.2: Money Laundering Process

2. Layering

Layering involves the separation of proceeds from illegal source using complex transactions designed to obscure the audit trail and hide the proceeds. The criminals frequently use shell corporations, offshore banks or countries with loose regulation and secrecy laws for this purpose. Layering involves sending the money through various financial transactions to change its form and make it difficult to follow. Layering may consist of several banks to bank transfers or wire transfers between different accounts in different names in different countries making deposit and withdrawals to continually vary the amount of money in the accounts changing the money's currency purchasing high value items (boats, houses cars, diamonds) to change the form of money-making it hard to trace.

3. **Integration**

Integration involves conversion of illegal proceeds into apparently legitimate business earnings through normal financial or commercial operations. Integration creates the illusion of a legitimate source for criminally derived funds and involves techniques as numerous and creative as those used by legitimate businesses. For e.g. false invoices for goods exported, domestic loan against a foreign deposit, purchasing of property and comingling of money in bank accounts.

II. Anti-Money laundering (AML) using Technology

Negative publicity, damage to reputation and loss of goodwill, legal and regulatory sanctions and adverse effect on the bottom line are all possible consequences of a bank's failure to manage the risk of money laundering. Banks face the challenge of addressing the threat of money laundering on multiple fronts as banks can be used as primary means for transfer of money across geographies. The challenge is even greater for banks using CBS as all transactions are integrated. With regulators adopting stricter regulations on banks and enhancing their enforcement efforts, banks are using special fraud and risk management software to prevent and detect fraud and integrate this as part of their internal process and daily processing and reporting.

III. Financing of Terrorism

Money to fund terrorist activities moves through the global financial system via wire transfers and in and out of personal and business accounts. It can sit in the accounts of illegitimate charities and be laundered through buying and selling securities and other commodities, or purchasing and cashing out insurance policies. Although terrorist financing is a form of money laundering, it does not work the way conventional money laundering works. The money frequently starts out clean i.e. as a 'charitable donation' before moving to terrorist accounts. It is highly time sensitive requiring quick response.

As per compliance requirements of PMLA, CBS software should include various type of reports which are to be generated periodically for filing with regulatory agencies. Further, management should do regular monitoring of these type of transactions on proactive basis and take necessary action including reporting to the regulating agencies.

5.5.3 Cyber Crimes

Cybercrime also known as computer crime is a crime that involves use of a computer and a network. The computer may have been used in committing a crime, or it may be the target. Cybercrimes is defined as: 'Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones.

The United Nations Manual on the Prevention and Control of Computer Related Crime classifies such crimes into following categories:

- Committing of a fraud by manipulation of the input, output, or throughput of a computer based system.
- Computer forgery, which involves changing images or data stored in computers,
- Deliberate damage caused to computer data or programs through virus programs or logic bombs,
- Unauthorized access to computers by 'hacking' into systems or stealing passwords, and,
- Unauthorized reproduction of computer programs or software piracy.
- Cybercrimes have grown big with some countries promoting it to attack another country's security and financial health.

Banking sector is prone to high risks by cyber criminals as banks deal with money and using technology, frauds can be committed across geographical boundaries without leaving a trace. Hence, CBS and banking software is expected to have high level of controls covering all aspects of cyber security.

5.5.4 Banking Regulation Acts

The Banking Regulation Act, 1949 is legislation in India that regulates all banking firms in India. Initially, the law was applicable only to banking companies. But in 1965, it was amended to make it applicable to cooperative banks and to introduce other changes. The Act provides a framework using which commercial banking in India is supervised and regulated.

The Act gives the Reserve Bank of India (RBI) the power to license banks, have regulation over shareholding and voting rights of shareholders; supervise the appointment of the boards and management; regulate the operations of banks; lay down instructions for audits; control moratorium, mergers and liquidation; issue directives in the interests of public good and on banking policy, and impose penalties. In 1965, the Act was amended to include cooperative banks under its purview by adding the Section 56. Cooperative banks, which operate only in one state, are formed and run by the state government. But, RBI controls the licensing and regulates the business operations. The Banking Act was a supplement to the previous acts related to banking.

RBI has been proactive in providing periodic guidelines to banking sector on how IT is deployed. It also facilitates banks by providing specific guidelines on technology frameworks, standards and procedures covering various aspects of functioning and computerization of banks in India. RBI also provides the technology platform for NEFT/ RTGS and other centralized processing from time to time.

I. Negotiable Instruments Act-1881 (NI Act)

Under NI Act, Cheque includes electronic image of truncated cheque and a cheque in the electronic form. The truncation of cheques in clearing has been given effect to and appropriate safeguards in this regard have been set forth in the guidelines issued by RBI from time to time.

A cheque in the electronic form has been defined as 'a mirror image' of a paper cheque. The expression 'mirror image' is not appropriate. It is perhaps not even the intention that a cheque in the electronic form should look like a paper cheque as seen in the mirror. Further, requiring a paper cheque being written first and then its mirror image or electronic image being generated does not appear to have been contemplated as the definition requires generation, writing and signature in a secure system etc. The expression, 'mirror image of' may be substituted by the expression, 'electronic graphic which looks like' or any other expression that captures the intention adequately.

The definition of a cheque in electronic form contemplates digital signature with or without biometric signature and asymmetric crypto system. Since the definition was inserted in the year)00), it is understandable that it has captured only digital signature and asymmetric crypto system dealt with under Section 3 of IT Act, 2000. Since IT Act, 2000 has been amended in the year 2008 to make provision for electronic signature also, suitable amendment in this regard may be required in NI Act so that electronic signature may be used on cheques in electronic form.

II. RBI Regulations

The **Reserve Bank of India (RBI)** was established on April 1, 1935 in accordance with the provisions of the Reserve Bank of India Act, 1934. The basic functions of the Reserve Bank as: 'to regulate the issue of Bank Notes and keeping of reserves with a view to securing monetary stability in India and generally to operate the currency and credit system of the country to its advantage." The Primary objective of BFS is to undertake consolidated supervision of the financial sector comprising commercial banks, financial institutions and non-banking finance companies. Some of the key functions of RBI are given here.

- **Monetary Authority:** Formulates implements and monitors the monetary policy with the objective of maintaining price stability and ensuring adequate flow of credit to productive sectors.
- **Regulator and supervisor of the financial system:** Prescribes broad parameters of banking operations within which the country's banking and financial system functions with the objective of maintaining public confidence in the system, protect depositors' interest and provide cost-effective banking services to the public.
- **Issuer of currency:** Issues and exchanges or destroys currency and coins not it for circulation with the objective to give the public adequate quantity of supplies of currency notes and coins and in good quality.

Banks provides various types of banking services and technology is used to provide these services. Earlier, Technology was one of the enablers but now, Technology has become the building block for providing all banking services.

III. Prevention of Money Laundering Act (PMLA)

Only relevant sections pertaining to the topic are discussed below:

<u>CHAPTER II OFFENCE OF MONEY-LAUNDERING</u>

<u>Section 3. Offence of money-laundering</u>

Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the 17 proceeds of crime including its concealment,

possession, acquisition or use and projecting or claiming it as untainted property shall be guilty of offence of money-laundering.

CHAPTER IV OBLIGATIONS OF BANKING COMPANIES, FINANCIAL INSTITUTIONS AND INTERMEDIARIES

Section 12. Reporting entity to maintain records.

(1) Every reporting entity shall—

(a) maintain a record of all transactions, including information relating to transactions covered under clause (b), in such manner as to enable it to reconstruct individual transactions;

(b) furnish to the Director within such time as may be prescribed, information relating to such transactions, whether attempted or executed, the nature and value of which may be prescribed;

(c) Omitted

(d) Omitted

(e) maintain record of documents evidencing identity of its clients and beneficial owners as well as account files and business correspondence relating to its clients.

[Note: Clauses (c) and (d) have been omitted]

(2) Every information maintained, furnished or verified, save as otherwise provided under any law for the time being in force, shall be kept confidential.

(3) The records referred to in clause (a) of sub-section (1) shall be maintained for a period of five years from the date of transaction between a client and the reporting entity.

(4) The records referred to in clause (e) of sub-section (1) shall be maintained for a period of five years after the business relationship between a client and the reporting entity has ended or the account has been closed, whichever is later.

(5) The Central Government may, by notification, exempt any reporting entity or class of reporting entities from any obligation under this Chapter.

Section 13. Powers of Director to impose fine.

(1) ***The Director may, either of his own motion or on an application made by any authority, officer or person, make such inquiry or cause such inquiry to be made, as he thinks fit to be necessary, with regard to the obligations of the reporting entity, under this Chapter.***

(1A) ***If at any stage of inquiry or any other proceedings before him, the Director having regard to the nature and complexity of the case, is of the opinion that it is necessary to do so, he may direct the concerned reporting entity to get its records, as may be specified, audited by an accountant from amongst a panel of accountants, maintained by the Central Government for this purpose.***

(1B) ***The expenses of, and incidental to, any audit under sub-section (1A) shall be borne by the Central Government.***

(2) ***If the Director, in the course of any inquiry, finds that a reporting entity or its designated director on the Board or any of its employees has failed to comply with the obligations under this Chapter, then, without prejudice to any other action that may be taken under any other provisions of this Act, he may—***

(a) ***issue a warning in writing; or***

(b) ***direct such reporting entity or its designated director on the Board or any of its employees, to comply with specific instructions; or***

(c) ***direct such reporting entity or its designated director on the Board or any of its employees, to send reports at such interval as may be prescribed on the measures it is taking; or***

(d) ***by an order, impose a monetary penalty on such reporting entity or its designated director on the Board or any of its employees, which shall not be less than ten thousand rupees but may extend to one lakh rupees for each failure.***

(3) ***The Director shall forward a copy of the order passed under sub-section (2) to every banking company, financial institution or intermediary or person who is a party to the proceedings under that sub-section.***

***Explanation -** For the purpose of this section, "accountant" shall mean a chartered accountant within the meaning of the Chartered Accountants Act, 1949 (38 of 1949).*

CHAPTER X MISCELLANEOUS

Section 63. Punishment for false information or failure to give information, etc.

(1) Any person willfully and maliciously giving false information and so causing an arrest or a search to be made under this Act shall on conviction be liable for imprisonment for a term which may extend to two years or with fine which may extend to fifty thousand rupees or both.

(2) If any person -

(a) being legally bound to state the truth of any matter relating to an offence under section 3, refuses to answer any question put to him by an authority in the exercise of its powers under this Act; or

(b) refuses to sign any statement made by him in the course of any proceedings under this Act, which an authority may legally require to sign; or

(c) to whom a summon is issued under section 50 either to attend to give evidence or produce books of account or other documents at a certain place and time, omits to attend or produce books of account or documents at the place or time,

he shall pay, by way of penalty, a sum which shall not be less than five hundred rupees but which may extend to ten thousand rupees for each such default or failure.

(3) No order under this section shall be passed by an authority referred to in sub-section (2) unless the person on whom the penalty is proposed to be imposed is given an opportunity of being heard in the matter by such authority.

(4) Notwithstanding anything contained in clause (c) of sub-section (2), a person who intentionally disobeys any direction issued under section 50 shall also be liable to be proceeded against under section 174 of the Indian Penal Code (45 of 1860).

<u>Section 70. Offences by companies</u>.

(1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made there under is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to the company, for the conduct of the business of the company as well as the company, shall be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:

Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

(2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made there under has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of any director, manager, secretary or other officer of any company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

<u>Explanation 1 -</u> For the purposes of this section -

(i) "company" means anybody corporate and includes a firm or other association of individuals; and

(ii) "director", in relation to a firm, means a partner in the firm.

<u>Explanation 2 -</u> For the removal of doubts, it is hereby clarified that a company may be prosecuted, notwithstanding whether the prosecution or conviction of any legal juridical person shall be contingent on the prosecution or conviction of any individual.

II. Information Technology Act

The Information Technology Act was passed in 2000 and amended in 2008. The ITA Rules were passed in 2011. The Act provides legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as ‘electronic commerce', which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government. The Act provides the legal framework for electronic governance by giving recognition to electronic records and digital signatures. It also deals with cyber-crime and facilitates electronic commerce. It also defined cyber-crimes and prescribed penalties for them. The Amendment Act 2008 provides stronger privacy data protection measures as well as implementing reasonable information security by implementing ISO 27001 or equivalent certifiable standards to protect against cyber-crimes.

For the banks, the Act exposes them to both civil and criminal liability. The civil liability could consist of exposure to pay damages by way of compensation up to 5 crores. There may also be exposure to criminal liability to the top management of the banks and exposure to criminal liability could consist of imprisonment for a term which would extend from three years to life imprisonment as also fine. Further, various computer related offences are enumerated in the aforesaid provisions which will impact banks. There have been many instances of 'phishing' in the banking industry whereby posing a major threat to customers availing internet banking facilities.

CBS is a technology platform which provides integrated interface for bank and its customers with access online, anytime and anywhere. Hence, it is prone to various types of cybercrimes and frauds which can be committed by staff, customers, vendors or any hacker/ outsider. The IT Act recognizes risks of information technology deployment in India, various types of computer-related offences and provides a legal framework for prosecution for these offences.

Some Definitions in IT Act

The IT Act, 2000 defines the terms Access in computer network in Section 2(a), computer in Section 2(i), computer network in Section (2j), data in Section 2(o) and information in Section 2(v). These are all the necessary ingredients that are useful to technically understand the concept of Cyber Crime.

2(a) "Access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;

2(i) "Computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

2(j) "Computer Network" means the interconnection of one or more Computers or Computer systems or Communication device through-

(i) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and

(ii) terminals or a complex consisting of two or more interconnected computers or communication device whether or not the interconnection is continuously maintained;

2(o) "Data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

2(v) "Information" includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche;

In a cyber-crime, computer or the data are the target or the object of offence or a tool in committing some other offence. The definition of term computer elaborates that computer is not only the computer or laptop on our tables, as per the definition computer means any electronic, magnetic, optical or other high speed data processing devise of system which performs logical, arithmetic and memory function by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network. Thus, the definition is much wider to include mobile phones, automatic washing machines, micro wave ovens etc.

A. Key Provisions of IT Act

Some of key provisions of IT related offences as impacting the banks are given here.

Section 43: Penalty and compensation 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 1[or computer resource];

(b) downloads, copies or extracts any data, computer database 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 database or any other programmes 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 authorized 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 there under;

(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;

(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

(j) steal, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage,

he shall be liable to pay damages by way of compensation to the person so affected.

Explanation - For the purposes of this section -

(i) "computer contaminant" means any set of computer instructions that are designed—

(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(b) by any means to usurp the normal operation of the computer, computer system, or computer network;

(ii) "computer database" means a representation of information, know-ledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

(iv) "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means;

(v) "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

Section 43A: Compensation for failure to protect data.

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining

reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Explanation - For the purposes of this section -

(i) ***"<u>body corporate</u>" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;***

(ii) ***"<u>reasonable security practices and procedures</u>" means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;***

(iii) ***"<u>sensitive personal data or information</u>" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.***

Section 65: 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 which may extend up to 2 lakh rupees, or with both. The explanation clarifies ‘Computer Source Code” means the listing of programme, Computer Commands, Design and layout and program analysis of computer resource in any form.

Section 66: Computer Related Offences

If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to 5 lakh rupees or with both.

Section 66-B: Punishment for dishonestly receiving stolen computer resource or communication device

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

Section 66-C: Punishment for identity theft

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Section 66-D: Punishment for cheating by personation by using computer resource

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Section 66-E: Punishment for violation of privacy

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

B. Sensitive Personal Data Information (SPDI)

Section 43A of the IT Amendment Act imposes responsibility for protection of stakeholder information by body corporate. The IT Act has a specific category, 'sensitive personal data or information,' which consists of password, financial information (including bank account, credit card, debit card or other payment details), physical, physiological and mental health conditions, sexual orientation, medical records, and biometric information. This legally obligates all stakeholders (i.e., any individual or organization that collects, processes, transmits, transfers, stores or deals with sensitive personal data) to adhere to its requirements.

One of the largest stakeholders of SPDI are include banks apart from insurance companies, financial institutions, hospitals, educational institutions, service providers, travel agents, payment gateway providers and social media platforms, etc. Hence, at a corporate level, every bank should develop, communicate and host the privacy policy of the bank. The policy should include all key aspects of how they deal with the personal information collected by the bank. To provide practical perspective of how compliance to the provisions of IT Act specifically relating to privacy and protection of personal information, the next section provides an overview of requirements of privacy policy of a bank.

C. Privacy Policy

Every bank deals captures Personal Information of customers as per definition of IT Act. Hence, it is mandatory to ensure security of personal information. This information must be protected by maintaining physical, electronic, and procedural safeguards by using appropriate security standards such as ISO 27001 to ensure compliance with regulatory requirements. Further, the employees of banks should be trained in the proper handling of personal information. Even when such services are outsourced, the vendor companies who provide such services are required to protect the confidentiality of personal information they receive and process. This aspect must be contractually agreed and the compliance of this monitored.

The specific information collected is to be confirmed with the customers. The type of information collected could be Non-Personal and Personal Information. For example, when the customer visits the website of the bank, information about the IP address of the device used to connect to the Internet is collected. Further, additional information such as browser used, browser version, operating system used is also collected, the use of cookies on visiting website and option to disable them has to be informed and provided to user.

The Personal Information provided by customer such as name, address, phone number, and email is collected and used by bank to offer new online experiences. In case of online bill payment, personal information about the transactions, and how customer interacts with third parties such as utility company or phone company is collected. The customer must be provided access to change information for their account or application by logging on to their account online or telephoning customer service. The customer should be able to control how their non-personal information is collected and used online.

SUMMARY

Banking is backbone of a country's economy which keeps the wheels of economy running. There are new products and services which are being provided by banks to meet the challenges of digital economy. Technology has become edifice for most of banking services which are provided increasingly in digital format rather than physical format. There are new forms of digital payment systems which are evolving continuously and being constantly pushed by government in the rush to digitization. The key differentiator among banks is the way technology is used to provide services in new ways and modes. Digitization gives rise to new risks which need to be mitigated by implementing right type of controls. Technology is used for enabling business processes. Hence, it is important to understand the business processes, work flow, business rules and related risks and controls.

A brief overview of impact of technology on business processes of banking and related risks and controls is provided. It covers various automated business processes of banking in terms of specific modules and functions. It also outlines the reliance on Internal Controls and how these are automated through various layers of technology. CBS is being increasingly used in banking sector. Hence, it is important to understand components and Architecture of CBS and impact of related risks and controls. The functioning of core modules of banking and Business process flow and impact of related risks and controls has been discussed. Specific distinction between General controls and application controls and sample listing of risk and control matrix has been provided to help understand how risks are integral in each aspects of business processes and how controls are to be embedded inside each layer and component of technology as required.

Reporting systems are most critical interface for users of software as they provide the processed information as required by various levels of management. These reports are used for monitoring performance and direct the enterprise for achieving objectives. In case of banks and specifically in CBS, there is huge volume of centralized data which is an abundant source for applying data analysis and infer insights for decision- making. The basic concepts of data analytics and business intelligence as primary tools for analyzing information for decision-making have been explained. Data analytics performed using technology can process large volumes of data across banks to provide patterns, hindsight, insights and foresights which are useful for analyzing not only the past and present and to predict the future.

Banking is highly regulated as it the prime driver of economy and deals with money which is prone to fraud. An overview of some of the regulatory and compliance requirements specifically applicable to automated environment such as CBS has been covered. Further, IT leads to new risks of Cybercrime due to increased availability of internal information system of bank through online mode. The key provisions of Information Technology Act such as computer-related offences, need to ensure security of information and protect Sensitive Personal Data Information have been briefly explained. There are new regulations such as Prevention of Money Laundering Act which mandate regulating flow of money through legal banking channels have been explained.

TEST YOUR KNOWLEDGE

Theoretical Questions

1. Distinguish between Application Server and Database Server.

   Refer Section 5.2.2.

2. Briefly explain core features of Core Banking Software. Refer Section 5.1.4.

3. Briefly explain major components of a CBS solution.

   Refer Section 5.2.1.

4. Explain the CBS IT environment. Refer Section 5.2.2.

5. What are the risks associated with CBS software?

   Refer Section 5.3.1.

6. What are the key provisions of Information Technology Act, 2000?

   Refer Section 5.5.4.

7. Briefly explain all the stages of Money Laundering and how banks are used in laundering money.

   Refer Section 5.5.2.

Multiple Choice Questions

1. Which of the following is not a core banking services?

   (a) Advances

   (b) Letters of Credit

   (c) Reporting

   (d) Deposits

2. Which of the following is an application control?

(a) Configuring system software

(b) Setting parameters in masters

(c) Transaction Logging

(d) Back up of data

3. Which of the following is a General control?

(a) Setting Database Security

(b) Edit checks

(c) Completeness check

(d) Format check

4. Which of the following is a core feature of CBS?

(a) On-line real-time processing

(b) Transactions are posted in batches

(c) Databases are maintained as per branch

(d) Loan processing is done at branch

5. Which of the following is one of the primary objective of implementing controls?

(a) All computer errors are prevented

(b) Frauds are detecting pro-actively

(c) Undesired events are prevented or detected and corrected

(d) Revenue targets are achieved

6. Which of the following best defines a risk?

(a) Undesired events are prevented

(b) Inherent vulnerabilities are identified

(c) Physical threats are documented

(d) Threat exploits vulnerability

7. Which of the following best defines Money Laundering?

(a) Converting proceeds of crime and projecting it as untainted property

(b) Tax Planning as per provision of IT Act

(c) Gifting immoveable property to relatives

(d) Transferring fixed deposit to employees

8. Which of the following is not computer related offence as per in IT Act, 2000?

(a) Identify theft

(b) Stealing of mobile

(c) Stealing computer resource

(d) Violation of privacy

9. What is the primary objective of SPDI?

(a) Protecting computer software

(b) Securing critical information

(c) Securing Personal Information

(d) Identifying sensitive information

10. Which of the following is a cybercrime?

(a) Breaking into ATM

(b) Physical theft at branch

(c) Software piracy

(d) Altering name in demand draft

Answers

1.	(c)	**2.**	(c)	**3.**	(a)	**4.**	(a)	**5.**	(c)	**6**	(d)
7.	(a)	**8.**	(b)	**9.**	(c)	**10.**	(c)				