CHAPTER 5

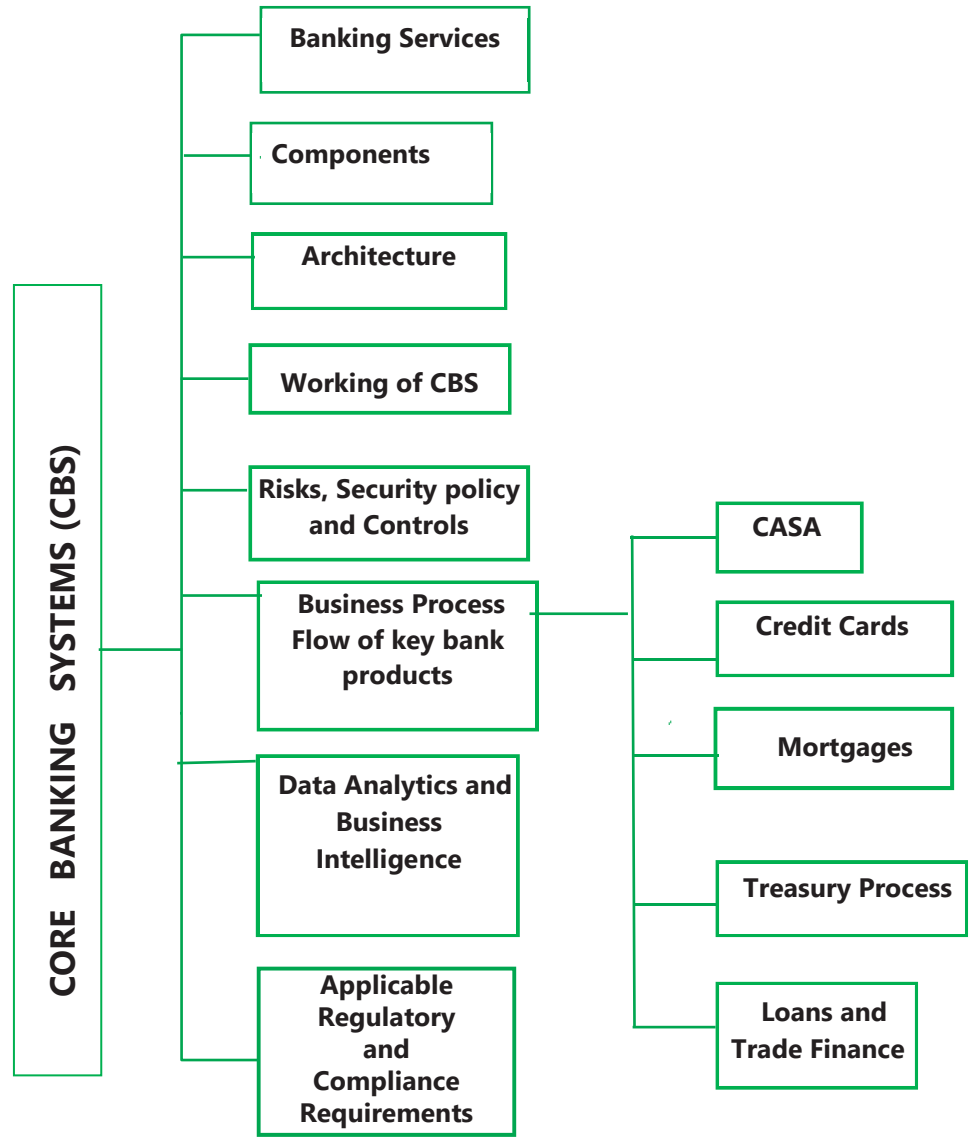
CORE BANKING SYSTEMS

LEARNING OUTCOMES

After reading this chapter, you will be able to -

- Understand components and architecture of Core Banking System (CBS) and impact of related risks and controls.
- Acknowledge 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, 2002 and
  - Information Technology Act, 2000.

CHAPTER OVERVIEW



5.1 OVERVIEW OF BANKING SERVICES

5.1.1 Introduction

Today India's banks compete globally at one level and at the same time provide various banking services to citizens of India staying even 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 are as follows:

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 playing 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 be left 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 the need of customers grew, so the need of businesses 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 thereby improving the overall efficiency and performance of its operations.

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 abled 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:

- As the custodian of large volumes of monetary items including cash and negotiable instruments, the banks need to ensure their physical security.
- The banks deal in large volume of data in terms of number, value, and variety of transactions.
- The banks need to operate through a wide network of their geographically dispersed branches and departments.
- There is an increased possibility of frauds as banks directly deals with money making. Therefore, its 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 made 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 other products.

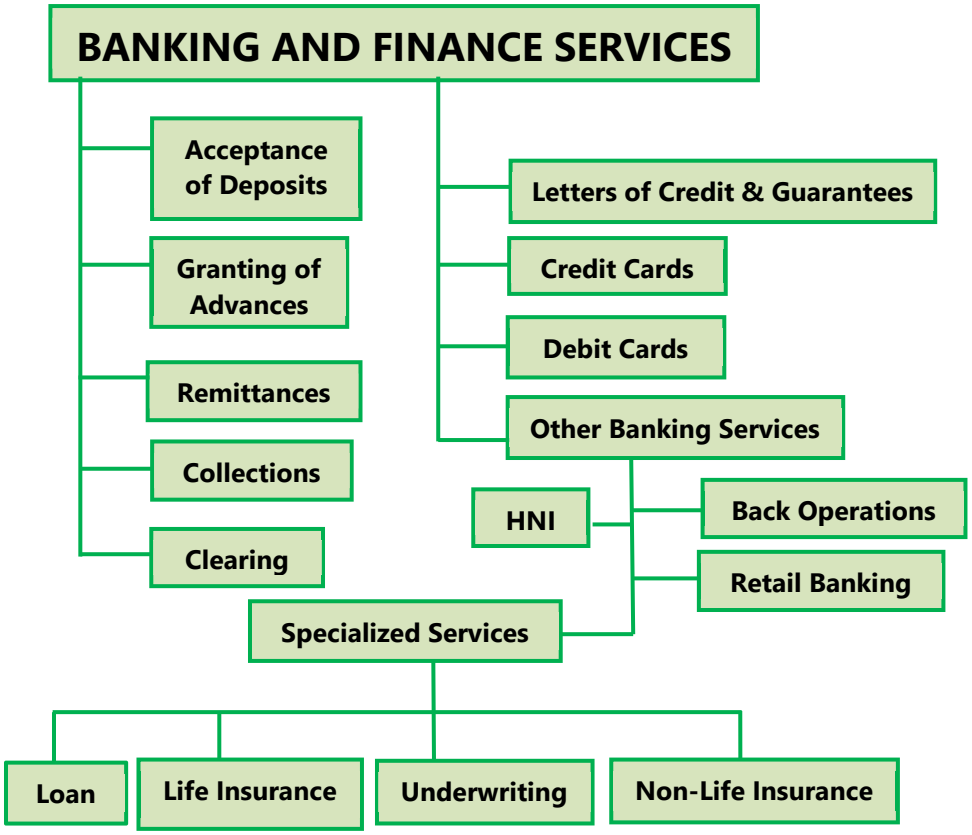


Fig. 5.1.1: Banking and Finance Services

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. Most common modes of remittance of funds are as follows:

- **Demand 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 demand drafts are handed over to the applicant.
- In case of **Mail Transfer (MT)**, no instrument (a document guaranteeing the payment of a specific amount of money, either on demand, or at a set time, with the payer named on the document, that includes cheques, drafts, bills of exchange, credit notes etc.) is handed over to the applicant. The transmission of the instrument is the responsibility of the branch. Generally, the payee of MT is an account holder of the paying branch.
- **Electronic Funds Transfer (EFT)** 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 the following:

  (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 24x7 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 (NSC), 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 charge 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 lodge, 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 for clearing which is an electronic method of fund transfer from one bank account to another.

ECS is generally used for bulk transfers performed by institutions for making payments like dividend, interest, salary, pension, etc. and takes two forms: **ECS Credit** or **ECS Debit**.

- In the case of **ECS Credit**, number of beneficiary accounts are credited by debiting periodically a single account of the bank. Examples of ECS Credit includes payment of amounts towards dividend distribution, interest, salary, pension, etc.
- In the case of **ECS Debit**, large number of accounts with the bank are debited for credit to a single account. Examples of ECS Debit includes tax collections, loan installment repayment, investments in mutual funds etc.

The Banks/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 customers are 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 that figure are explained below:

- **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 for personal use. E.g. Debit cards, Personal loans, Mortgages etc.
- **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.
- **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.
    - **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, an underwriter checks the borrower's ability to repay the loan based on an analysis of his/her credit history, value of collateral provided 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.
- ***Non-life Insurance:*** ***Insurance contracts that do not come under the ambit of life insurance are called Non-life or General Insurance. As the tangible assets like home, vehicle etc. are susceptible to damages, the general insurance provides protection against unforeseeable contingencies like loss of the asset due to fire, marine, motor, accident etc.***

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 System/Solution (CBS) refers to a common IT solution wherein a central shared database supports the entire banking application. It allows the customers to use various banking facilities irrespective of the bank branch location. The characteristics of CBS are as follows:

- CBS is a 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.
- There is a common database in a central server located at a Data Center, which gives a consolidated view of the bank's operations.
- 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.
- All branches of bank function as delivery channels providing services to its customers.
- A CBS software enables integration of all third-party applications including in-house banking software to facilitate simple and complex business processes.

Example 5.1: Some CBS software are given below. These are only illustrative and not exhaustive.

- **Finacle:** It is a core banking software suite developed by Infosys that provides universal banking functionality covering all modules for banks covering all banking services.
- **FinnOne:** This is a 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:** It is an automated, comprehensive, integrated, interoperable, and modular solution developed by Oracle Financial Services that enables banks to manage evolving customer expectations.
- **BaNCS:** It is a customer-centric business model which offers simplified operations comprising loans, deposits, wealth management, digital channels and risk and compliance components.
- **bankMate:** It is a full-scale banking solution which is scalable and integrated e-banking system 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 brain (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:

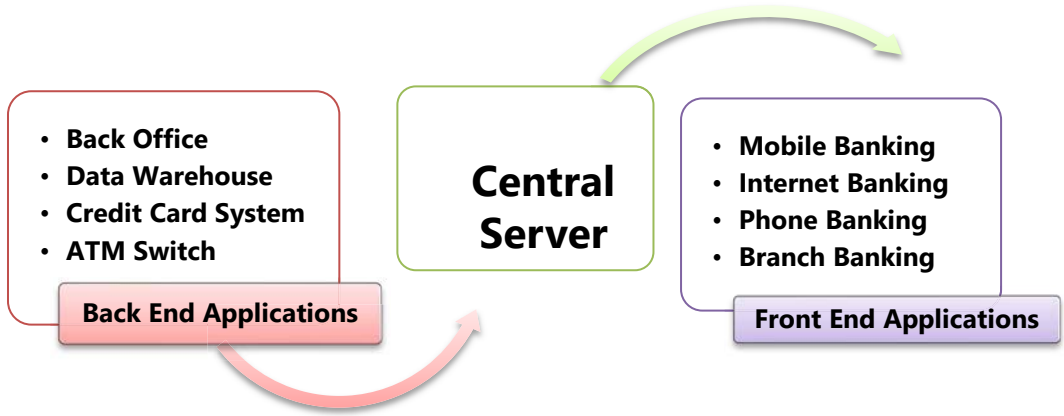


Fig. 5.1.2: Key Modules of CBS

We may recall from Chapter 2 that the **Front End** is a part of the overall application which interacts with the user who is using the software whereas the **Back End** is a part of the overall software that does not interact with the user but interact with front end only. 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, data warehouse, ATM switch, mobile banking, internet banking, phone banking and credit-card system etc. are all connected and related transactions are interfaced with the central server and are explained below:

- **Back Office:** 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.
- **Data Warehouse:** 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.

- **Credit-Card System:** 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.
- **Automated Teller Machines (ATM):** An Automated Teller Machine 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.
- **Central Server:** 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 at 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.
- **Mobile Banking/Internet Banking and Phone Banking:** Mobile Banking and Internet banking are two sides of the same coin. The screens have changed, the sizes have become smaller, and banking has become simpler. Mobile banking is a much latest entrant into the digital world of banking.
    - **Internet Banking** 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 accessed through any browser. 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.

- **Mobile Banking** is a service provided by a bank or other 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. The app needs to be downloaded to utilize this facility. Mobile banking is usually available on a 24-hour basis.
- **Phone Banking:** 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 an account is one of the basic perquisites 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.

- **Branch Banking:** 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 key functions like creating manual documents capturing data required for input into software; internal authorization; initiating Beginning-Of-Day (BOD) operations and 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 and deposits, customer records, balance of payments and withdrawal. Normal core banking functions 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).
- Real time seamless merging of data from the back office and self-service operations.
- Significant reduction in the errors which occurred due to duplication of entries.
- 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.
- Lesser operational cost due to less manpower usage.
- Automatic processing of standing instructions.
- Centralized interest applications for all accounts and account types.
- Anytime, anywhere access to customers and vendors.
- Banking access through multiple channels like mobile, web etc.

5.2 COMPONENTS AND ARCHITECTURE OF CBS

5.2.1 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. 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 (example 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.

B. 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, an accounting process being centralized at the centralized data center is updated at the centralized database.

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 file is called Positive Balance File (PBF). This ensures not only continuity of ATM operations but also confirms that the Central database is always upto 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 username and passwords of all the internet banking customers. IBCS software stores the name and password of the entire internet banking customers. 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 username and password.

E. Internet Banking Application Server(IBAS)

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.

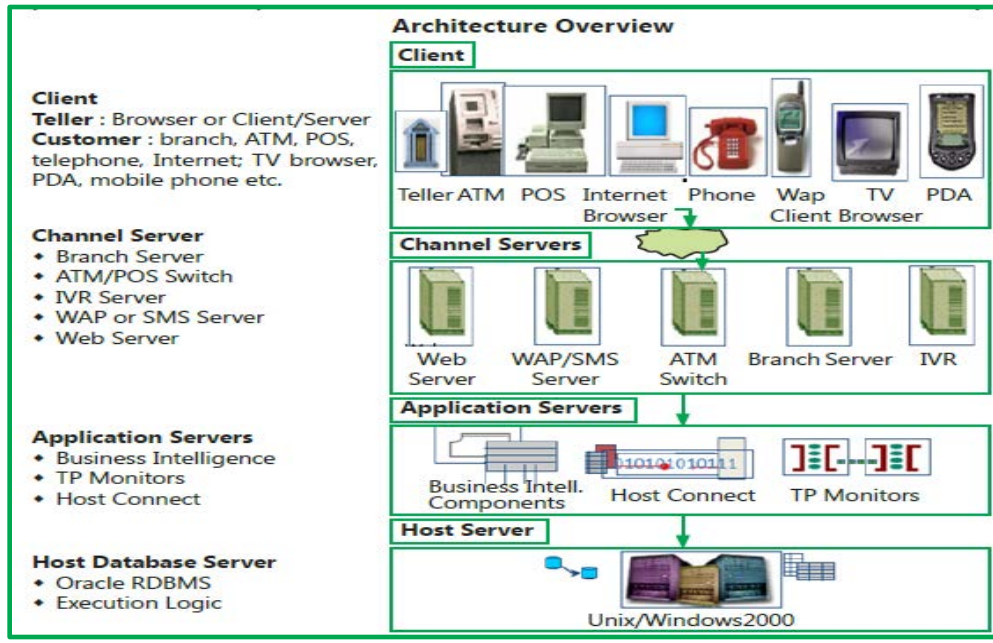


Fig. 5.2.1: CBS IT Environment

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 and hence often used to increase the speed and managing network bandwidth. In some cases, the proxy may alter the client's request or the server's response for various purposes. It serves as an intermediary between the users and the websites they browse for.

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.

5.2.2 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). With the introduction to core banking systems, a customer is not only having accessibility with the branch but to the bank.

The key technology components of CBS are as follows:

- **Database Environment:** This consists of the centrally located database servers that store the data for all the branches of the bank which includes customer master data, interest rates, account types etc. Whenever a customer requests for a particular service to be performed, the application server performs a particular operation it updates the central database server. The databases are kept very secure to prevent any unauthorized changes.
- **Application Environment:** In general, Application environment consist of the application servers that host the different core banking systems like Flex Cube, bankMate etc. and is centrally used by different banks. The access to these application servers will generally be routed through a firewall.
- ***Cyber Security: Comprehensive Cyber Security Framework is prescribed by RBI for Banks to ensure effective information security governance. Some key features of Cyber Security Framework as prescribed by are RBI for banks are as under:***

(i) ***Network Security and Secure Configuration: The following key measure are required to be implemented:***

- ***Multi-layered boundary defense through properly configured proxy servers, firewalls, intrusion detection systems to protect the network from any malicious attacks and to detect any unauthorized network entries.***
- ***Different LAN segments for in-house/onsite ATM and CBS/branch network to confirm the adequacy of bandwidth to deal with the volume of transactions so as to prevent slowing down and resulting in lower efficiency.***
- ***To ensure secure network configuration; proper usage of routers, hubs and switches should be envisaged.***
- ***Periodic security review of systems and terminals to assess the network's vulnerability and identify the weaknesses.***
- ***Identification of the risks to ensure that risks are within the bank's risk appetite and are managed appropriately.***

(ii) ***Application Security: Full-fledged Security policy to ensure Confidentiality, Integrity and Availability (CIA) of data and information needs to be development and implemented covering following key features:***

- ***Implementation of bank specific email domains (example, XYZ bank with mail domain xyz.in) with anti-phishing (security measures to prevent steal of user data) and anti-malware software (software tool/program to identify and prevent malicious software/malware from infecting network) with controls enforced at the email solution.***
- ***Two factor authentication, an extra step added to the log-in process, such as a code sent to user's phone or a fingerprint scan, that helps verify the user's identity and prevent cybercriminals from accessing private information.***
- ***Implementation of Password Management policy to provide guidance on creating and using passwords in ways that maximize security of the password and minimize misuse or theft of the password.***
- ***Effective training of employees to educate them to strictly avoid clicking any links received via email.***
- ***Proper reporting mechanism to save the banks from the effects of misconduct – including legal liability, lasting reputational harm, and serious financial losses.***
- ***Required to conduct effective due diligence and oversight to thoroughly assess the credentials of vendors/third party service providers/partners and making non-disclosure and security policy compliance agreements mandated for them.***
- ***Effective change management process to record/ monitor all the changes that are moved/ pushed into production environment.***
- ***Robust configuration management processes to register changes to business applications, supporting technology, service components and facilities.***
- ***Incident response and management mechanism to take appropriate action in case of any cyber security incident with well written incident response procedures elaborating the roles of staff handling such incidents.***
- ***Capturing of the audit logs pertaining to user actions and an alert mechanism to monitor any change in the log settings.***

- ***Continuous surveillance to stay regularly updated on the latest nature of emerging cyber threats.***

(iii) **Data Centre and Disaster Recovery Centre:** The core banking systems consist of a Data Centre which includes various application servers, database servers, web servers etc. and various other technological components. The bank should adopt full-fledged documentation and prepare necessary manuals dealing with the disaster recovery procedures. Arrangements for alternate connectivity of the banks with the data center should be established whenever there is a disruption in the primary connectivity. Proper awareness should be created among the employees through periodic trainings and mock drills.

(iv) **Online Transaction monitoring for fraud risk management:** Risk evaluations are carried out and considering the risk profile and other regulatory requirements of the bank, effective monitoring should be done as a part of managing fraud risk management across all delivery channels. There are also methods that facilitate fraud reporting in CBS environment. Proper alert system should be enabled to identify any changes in the log settings and the audit logs pertaining to user actions are captured.

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. It ensures various interfaces like payment channels, ATM, mobile/internet banking, Point of Sale (PoS) capability are readily available.
- **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 for banks which is complex and expensive. CBS has built-in and regularly updated regulatory platform which will ensure compliance by providing periodic regulatory and compliance reports required for the day-to-day operations of the bank.
- **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.

5.2.3 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.

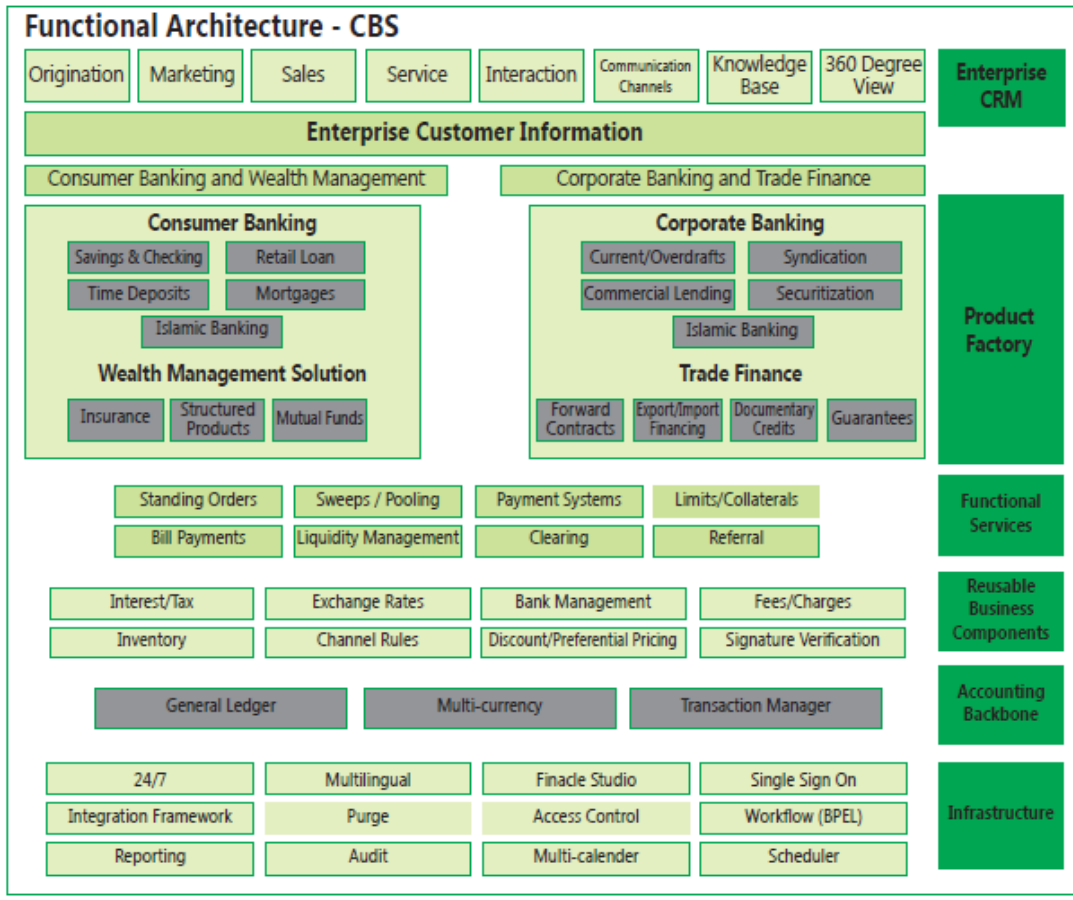


Fig. 5.2.2: Functional Architecture of CBS[1] (Illustrative)

[1] Source: Finacle

5.2.4 Internet Banking Process

- The customer applies to the bank for such internet banking 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, a browser like Internet Explorer, Firefox or Google 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 (IBAS) which in turn accesses the Internet Banking Database Server (IBDS). 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 Application Server (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 password change, balance inquiry, fund transfer, request for cheque book, stop payment, copy of statement of account and 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 For example- the statement of account from the central database server is made available to the Internet Banking Database Server (IBDS). The IBCS then sends the data to the IBAS. The IBAS then sends the same to the web browser (e.g. 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 like, 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 customer 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 website, 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 to enter password as OTP (One Time Password) received on mobile, to complete the transaction. After this, the customer is redirected to merchant site.

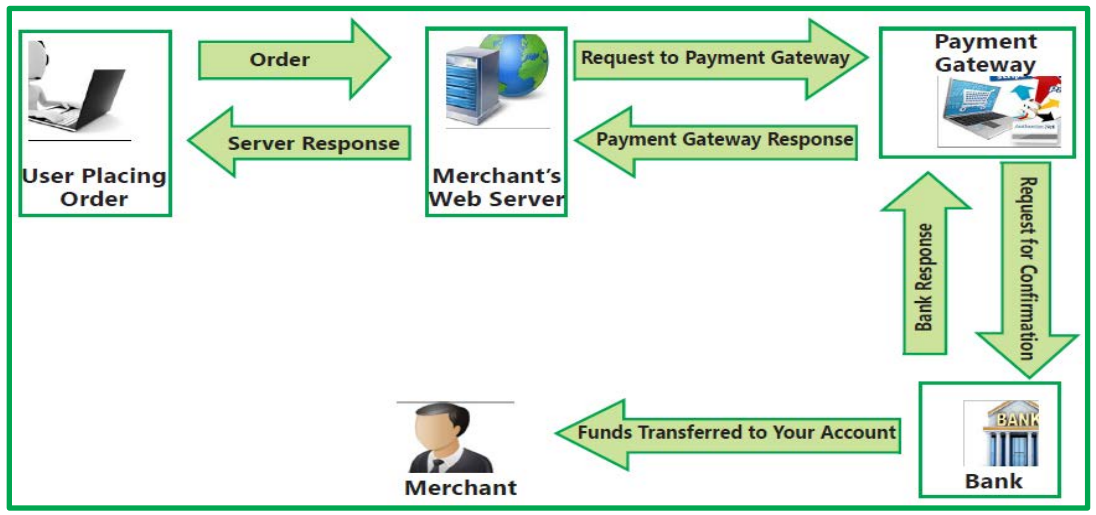


Fig. 5.2.3: e-Commerce Transaction flow for approval of payments

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. Suggest the appropriate technical steps to be taken by the management of the bank.

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 which is scalable and where different interfaces are readily available 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 deployments 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

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.

(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. For example- Inadequate audits, improper management, ineffective internal control procedures etc. The components of operational risk include transaction processing risk, information security risk, legal risk, compliance risk and people risk and necessarily excludes business risk and strategic risk.

- **Transaction Processing Risk** arises because faulty reporting of important market developments to the bank management may occur due to errors in entry of data for subsequent bank computations.
- **Information Security Risk** comprises the impact to an organization and its stakeholders that could occur due to the threats and vulnerabilities associated with the operation and use of information systems and the environments in which those systems operate. Data breaches can cost a bank its reputation, customers can lose time and money and above all their confidential information.
- **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.

- **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.
- **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.

(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. Non repayment of loans to the lending bank, constant defaults etc. results in huge non-performing assets which pave way for credit risks. Since bank and borrower usually signs a loan contract, credit risk can be considered as 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. For example - Reduction in the share price of the bank, loss incurred in major equity investment, wide fluctuation in interest rates etc. 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, new mergers or acquisitions or changing demand of customers.

(e) **IT Risk:** Once the complete business is captured by technology and processes are automated in CBS; the staff of the bank, customers, and management are completely dependent on the Data Centre (DC) of the bank. From a risk assessment and coverage point of view, it is critical to ensure that a 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 so that accountability can be fixed and unwanted changes to the data can be prevented.

- **Authorization process:** What is the authorization process, if anybody with access to the CBS, including the customer himself, can enter data directly. 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.
- **Maintaining response time:** Maintaining the interfacing software and ensuring optimum response time and up time can be challenging.
- **User Identity Management:** This could be a serious issue. Some banks may have more than 5000 users interacting with the CBS at once and therefore every user's identity and his/her level of access to a particular system need to be verified.
- **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.
- **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.
- **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 following sub-processes:

- **Information Security Policies, Procedures and practices:** This 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. Unauthorized access to information often occurs due to improperly understood poor or unorganized security practices. For example – Non-disclosure agreement with employees, vendors etc., KYC procedures for security.
- **User Security Administration:** This 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:** This 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. For example – Event Logging.
- **Database Security:** This refers to various aspects of implementing security for the database software. For example - Role based access privileges given to employees.

- **Operating System Security:** This refers to security for operating system software which is installed in the servers and systems which are connected to the servers.
- **Network Security:** This refers to how security is provided at various layers of network and connectivity to the servers. For example - Use of virtual private networks for employees, implementation of firewalls etc.
- **Physical Security:** This refers to security implemented through physical access controls. For example - Disabling the USB ports.

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	System owners authorize the nature and extent of user access privileges, and such

use, modification or denial of service in the system.	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 and ensuring compliance with the applicable laws and regulations. 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' Environment

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.

Example 5.2: Examples of Internal controls in bank branch are given below:

- 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.
- Effective internal audit should be carried out and any control deficiencies noted should be directly communicated to the senior management.

(b) IT Controls in Banks

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

- 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) Controls in Banks' Application Software

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**.

(Details of concepts of Configuration, Masters, Transactions have already been discussed in Chapter 1 in detail).

Example 5.3: 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 and its management; and
- Password Management

Example 5.4: 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.

Example 5.5: Transactions - Some examples of transactions in the context of CBS software are given here:

- **Deposit transactions:** Opening of account, deposits, withdrawals, interest computation, etc.

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

Example 5.6: 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; and
- 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 computed correctly. Digits are rounded off appropriately and 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 ((Non Resident External /Ordinary)accounts on change in residence status may result in regulatory non-compliance and undue benefits to customers.	On change of Customer status from NRI (Non Resident Indian)/ 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 Non-Performing Asset (NPAs are recorded on a bank's balance sheet after a prolonged period of non-payment by the borrower). 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 ownership.

5.4 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.

5.4.1 Business process flow of Current and Savings Accounts (CASA)

(a) Process Flow of CASA facility (as shown in the Fig. 5.4.1)

(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 (RM) on basis of the request made by the customer.

(ii) Once the potential customer agrees for availing the facilities/products of the bank, the RM 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/Saving 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.

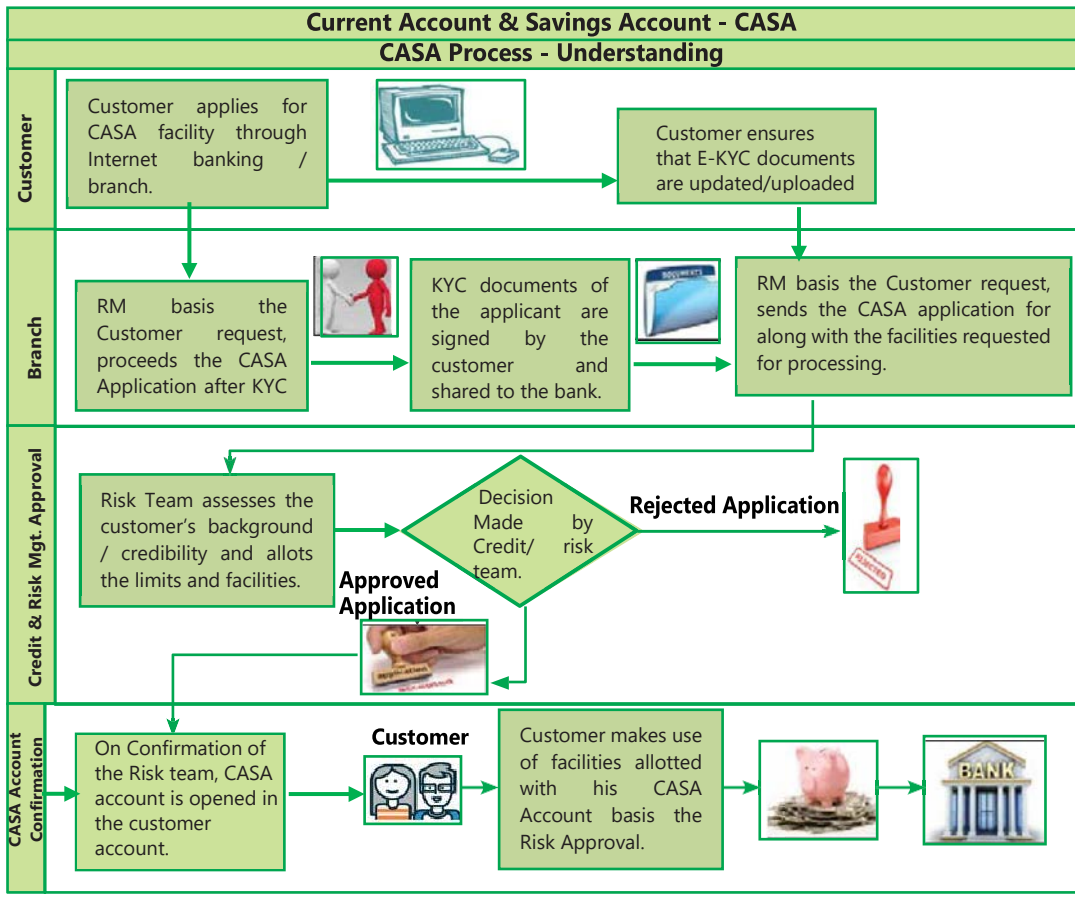


Fig. 5.4.1: CASA Process

(b) Risks & Controls around the CASA Process (discussed in the Table 5.4.1)

Table 5.4.1: Risks and Controls around the CASA Process

Risk	Key Controls
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.
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.
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.
Inaccurate interest/charge being calculated in CBS.	Interest on fund-based facilities is automatically calculated in the CBS as per the defined rules.
Unauthorized personnel approving the CASA transaction in CBS.	Segregation of Duties (SoD) to be maintained between the initiator and authorizer of the transaction for processing transaction in CBS.
Inaccurate accounting entries generated in CBS.	Accounting entries are generated by CBS based on the facilities requested by the customer and basis defined configurations for those facilities in CBS.

5.4.2 Business Process flow of Credit Cards

(a) Process Flow of Issuance of Credit Card Facility (as shown in the Fig. 5.4.2)

(i) Either the customer approaches the Relationship Manager(RM) 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 RM 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.

(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.

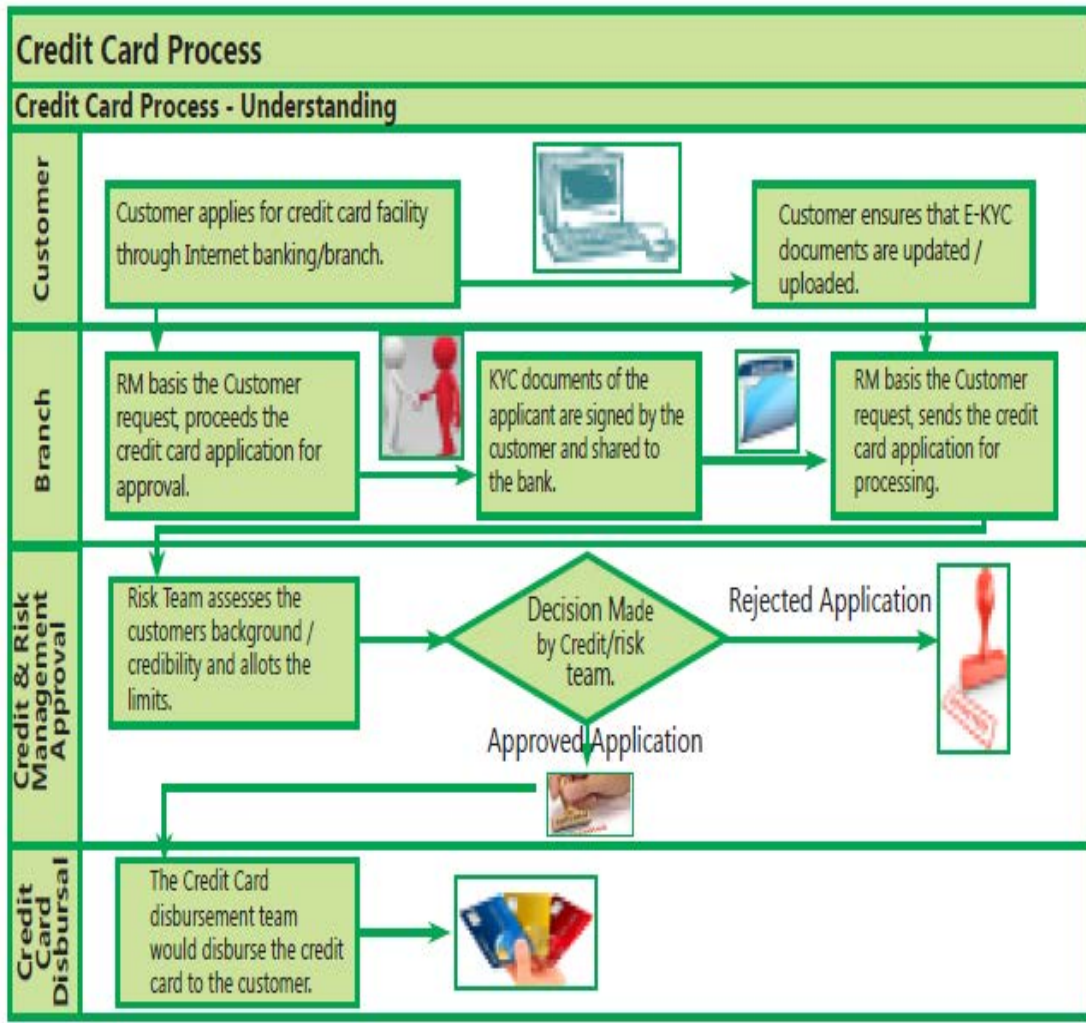


Fig. 5.4.2: Process Flow of Issuance of Credit Card Facility

(b) Process Flow of Sale - Authorization process of Credit Card Facility (as shown in the Fig. 5.4.3)

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

(ii) PoS will process the transaction only once the same is authenticated.

(iii) The PoS 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 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. 5.4.3)

(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.

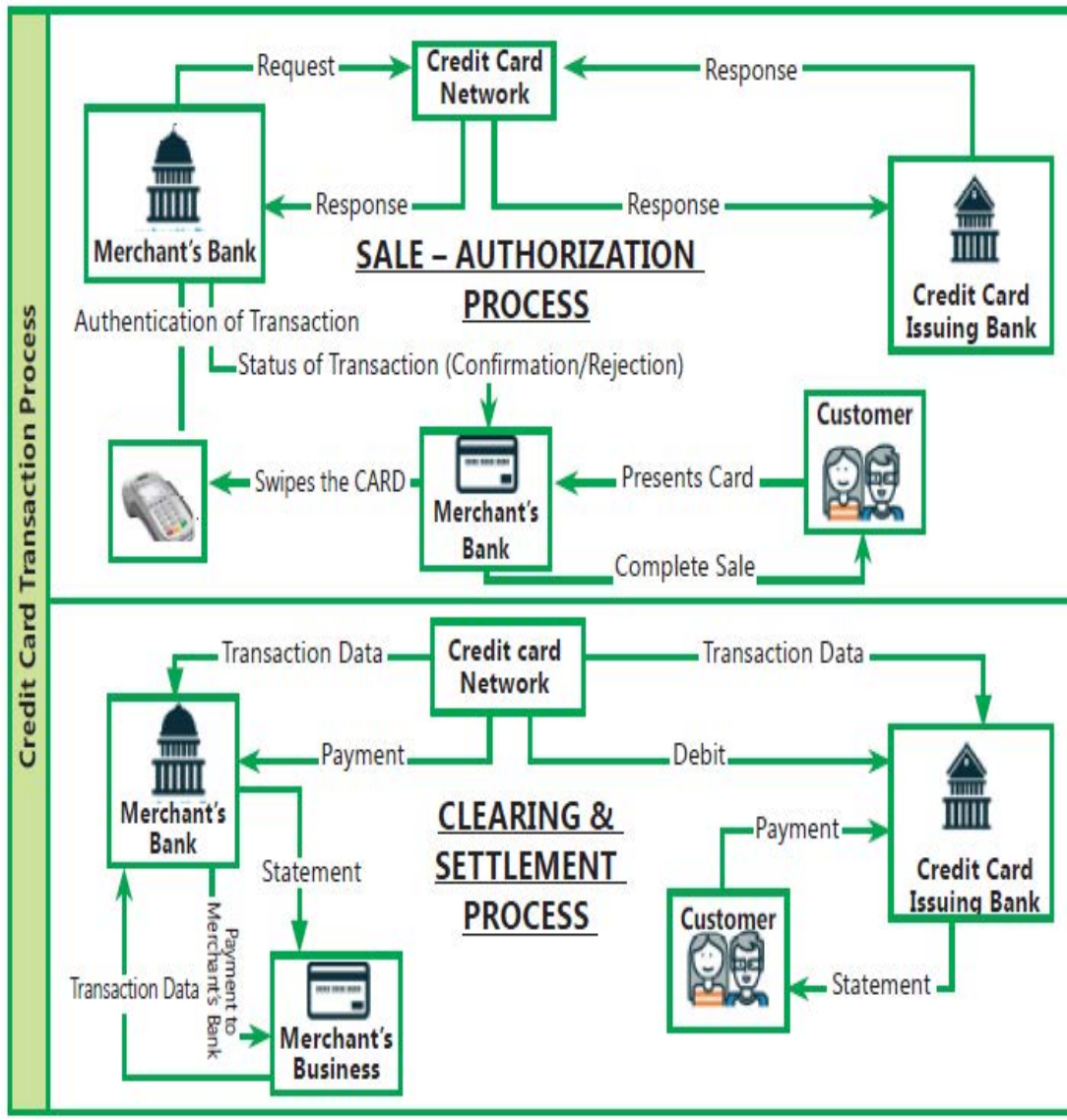


Fig. 5.4.3: Process Flow of Sale - Authorization and Clearing & Settlement of Credit Card Facility

(d) Risks and Controls around the Credit Card Process (Refer Table 5.4.2)

Table 5.4.2: Risks and Controls around the Credit Card Process

Risks	Key Controls
Credit Line setup is unauthorized and not in	The credit committee checks that the Financial Ratios, the Net-worth, the Risk factors and its

line with the bank's policy.	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.
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.
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, SoD 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.
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.
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.
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.

5.4.3 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.

Mortgage loans are conventionally the loans that one can use to buy or refinance a home. Due to the evolution in Banking industry, various other Mortgage Loans like Loan against residential property, Loan against commercial property, Loan against agricultural property, Loan against property etc. now exist apart from the ones that are discussed above.

(b) Process Description (as shown in the Fig. 5.4.4)

(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 and 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 approaches the bank for a mortgage and relationship manager/loan officer explains the customer about home loan and its various features. Customer fills the 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 will send them back to lender operations team.

(ix) Once the 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 activities 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.

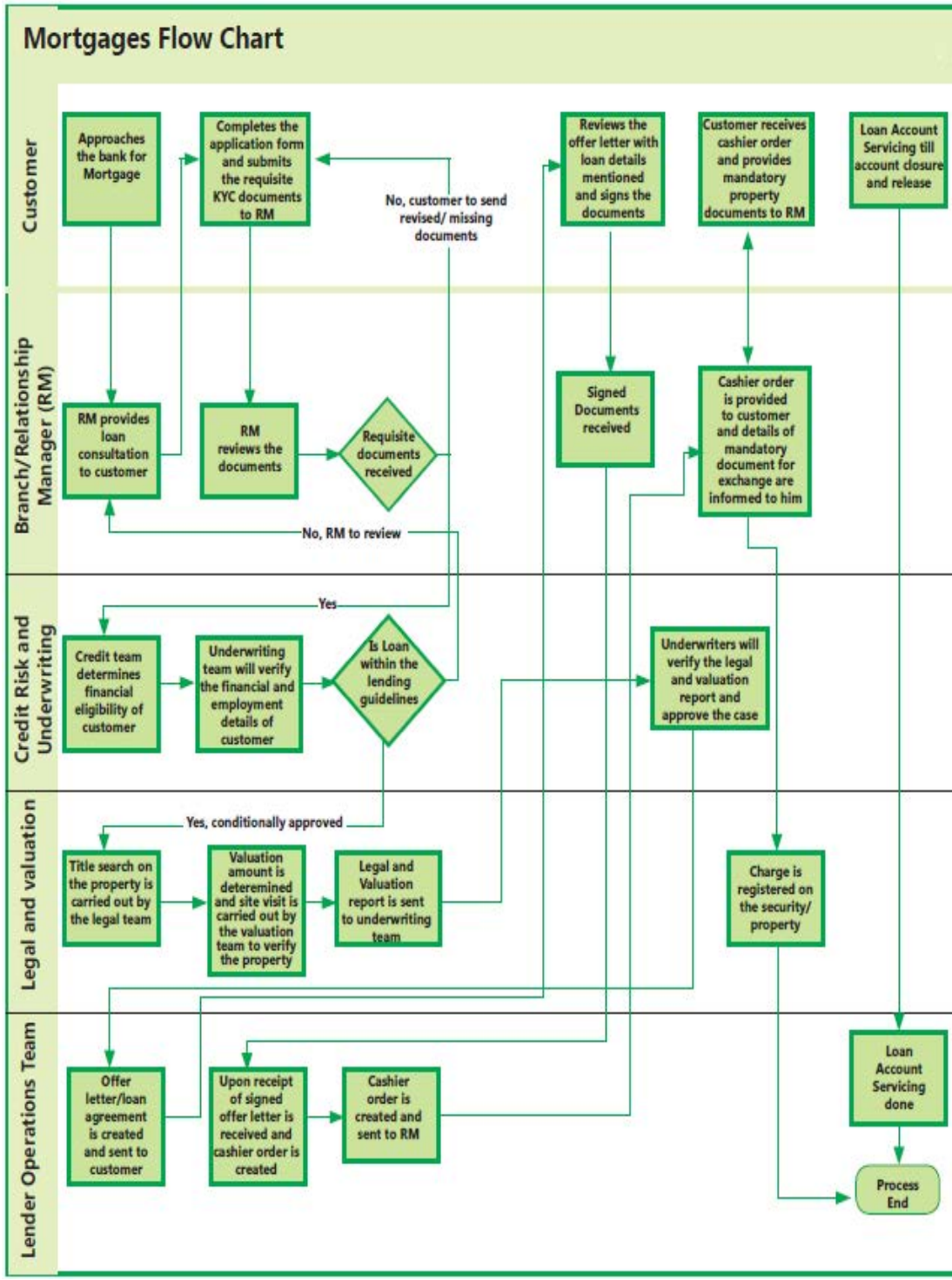


Fig. 5.4.4: Business process flow of Mortgages

(c) Risk & Controls around the Mortgage Process (discussed in the Table 5.4.3)

Table 5.4.3: Risk & Controls around the Mortgage Process

Risks	Key Controls
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.
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.
Interest amount is in- correctly calculated and charged.	Interest amount is auto calculated by the core banking application basis loan amount, RoI and tenure.
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.

5.4.4 Business Flow of Treasury Process

Investments Category are Government Securities (GSec), shares, other investments such as Commercial Papers, Certificate of Deposits, Security Receipts, Pass 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:

(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' Trading system, telephonic conversation, brokers or any other private channel

with the respective counterparty. 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 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, input into regulatory reporting producing the financial results and analysis and budget forecasts for the treasury business unit. 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 (that refers to a bank account held by a bank in 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 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 (SoD) 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. 5.4.5.

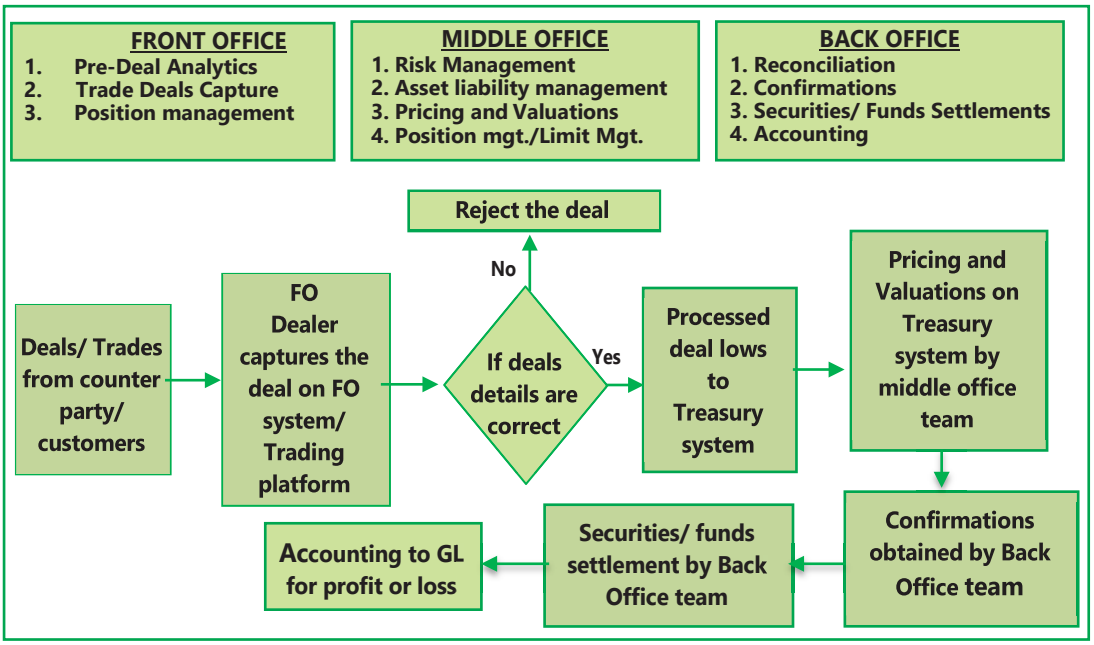


Fig. 5.4.5: Process Flow for Bank Treasury Operations

(c) Risk & Controls around the Treasury Process: (Listed in the Table 5.4.4)

Table 5.4.4: Risk & Controls around the Treasury Process

Risks	Key Controls
Unauthorized securities setup in systems such as Front office/Back office.	Appropriate SoD and review controls around securities master setup/ amendments.
Inaccurate trade is processed.	Appropriate SoD and review controls to ensure the accuracy and authorization of trades.

Unauthorized confirmations are processed.	Complete and accurate confirmations to be obtained from counter-party.
Insufficient Securities available for Settlement.	Effective controls on securities and margins.
Incomplete and inaccurate data flow between systems.	Inter-system reconciliations, Interfaces and batch processing controls.
Insufficient funds are available for settlements.	Controls at Clearing Corporation of India Limited (CCIL) / National Electronics Funds Transfer (NEFT) / Real Time Gross Settlement (RTGS) settlements to ensure the margin funds availability and the timely funds settlements.
Incorrect Nostro payments processed.	Controls at Nostro reconciliation and payments. (Nostro A/c refers to an account that a bank holds with a foreign bank in the currency of that country where the funds are held).

5.4.5 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 involve Cash Credits/Overdrafts, Demand Loans/Term loans and Bill Discounting.

(ii) Non-Fund Based Credit Facilities: In this type of credit facility, the banks' funds are not lent to the customers and 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 (Refer Table 5.4.5).

(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 (RM) 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 RM requests 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 documents, 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 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 5.4.5: Summary of Credit and Non-Credit Facilities

Product	Income for banks	Accounting of Income
Cash Credit/ Overdraft	Interest on Cash Credits/Overdraft balances.	Interest accrued on daily basis at the agreed rates.
Demand Loans/Term Loans	Interest on Demand Loans/ Term Loan.	Interest accrued on daily basis at the agreed rates.
Bill Discounting	Discounting Income	Interest accrued on daily basis at the agreed rates.
Bank Guarantee	Commission	Commission accrued over the tenure of the bank guarantee.
Letter of Credit	Commission Income	Commission accrued over the tenure of the bank guarantee.

(b) Process flow for Fund based loans (Fig. 5.4.6)

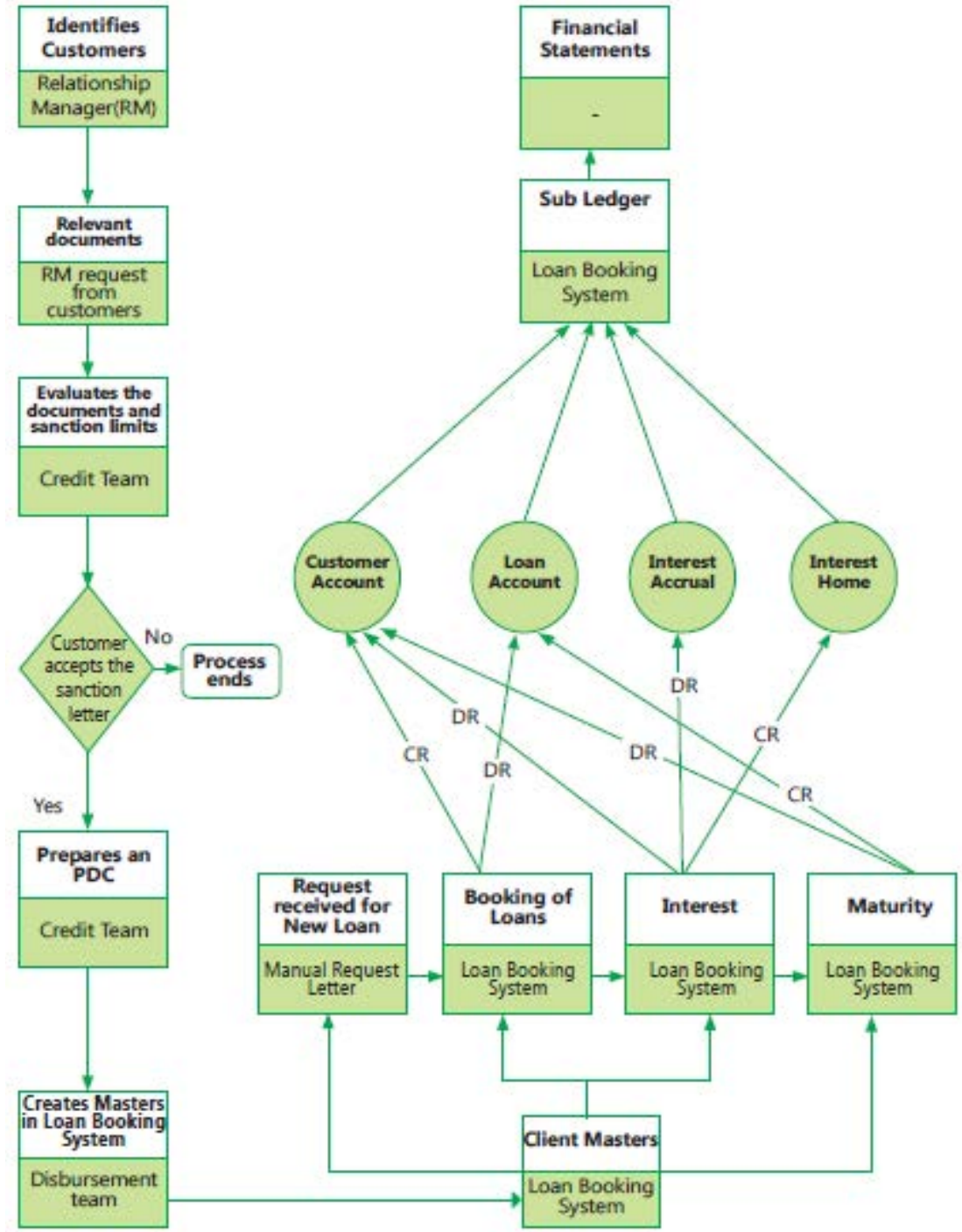


Fig. 5.4.6: Process Flow for Fund based Loans

(c) Process flow for Non-fund based loans (Fig. 5.4.7)

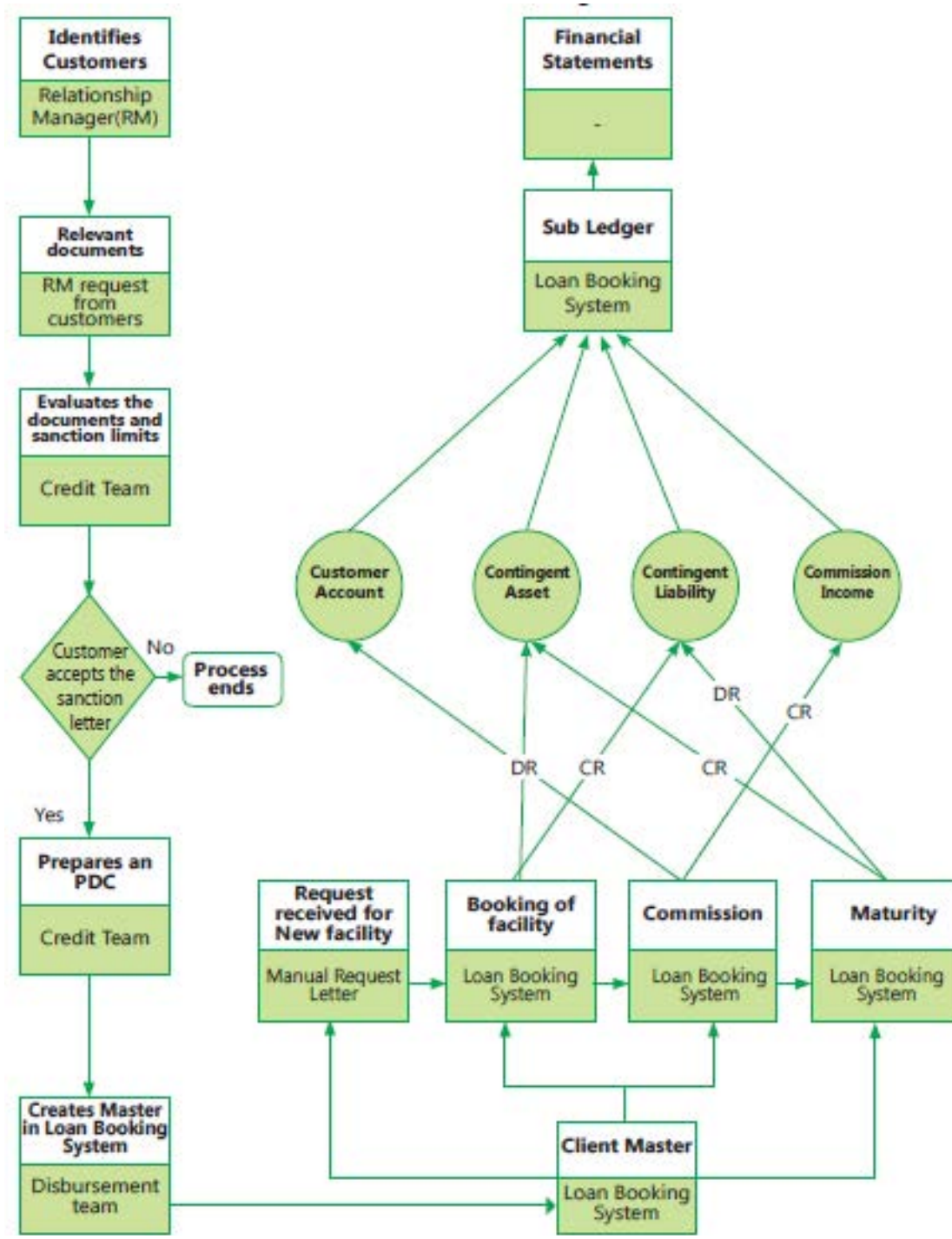


Fig. 5.4.7: Process Flow for Non - Fund based Loans

(d) Risk and Controls in the Loans and Advances Process: These are provided in the Table 5.4.6.

Table 5.4.6: Risk & Controls in the Loans and Advances Process

Risk	Key Controls
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.
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.
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.
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.
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.
Facilities/Loan's granted may be unauthorized/in-appropriate.	SoD 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.
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.

5.5 REPORTING SYSTEMS AND MIS, DATA ANALYTICS AND BUSINESS INTELLIGENCE

(The fundamental concepts of these topics are elaborately provided in the earlier Chapter 2 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 regulations, 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 that 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 in 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.

5.6 APPLICABLE REGULATORY AND COMPLIANCE REQUIREMENTS

5.6.1 Impact of Technology in Banking

The following Fig. 5.6.1 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 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.

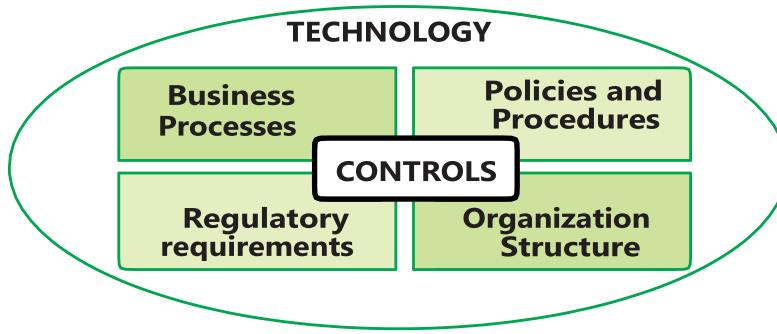


Fig. 5.6.1: Technology and Business Process Components

5.6.2 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. It 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. 5.6.2)

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. In this stage, the illegal funds or assets are first brought into the financial system.

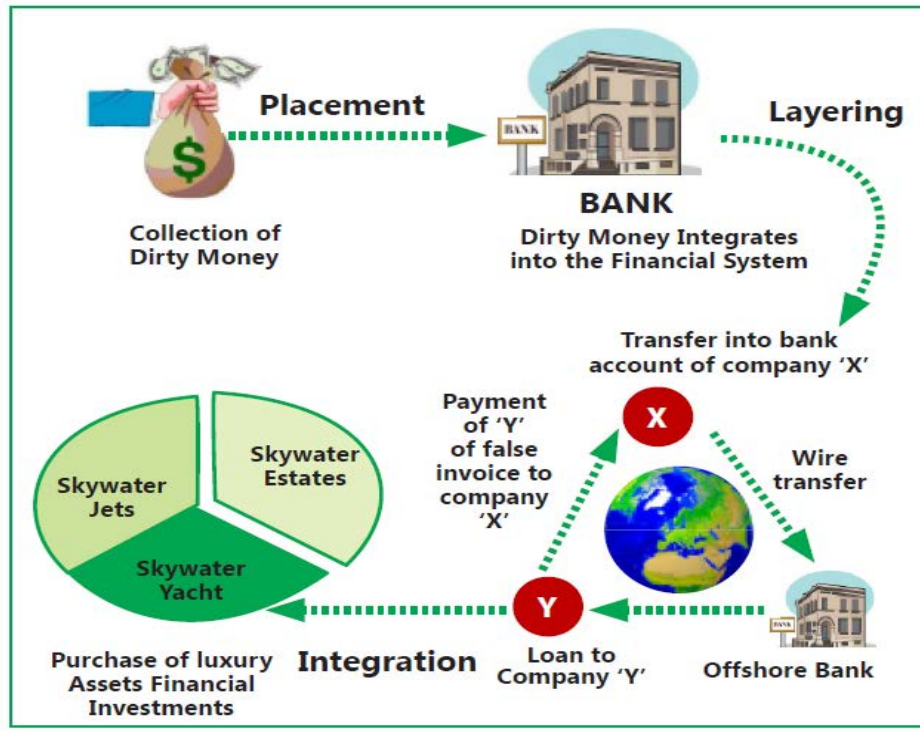


Fig. 5.6.2: Money Laundering Process

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 bank-to-bank transfers or wire transfers between different accounts in different names in different countries, making

deposits 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. This step is quite complex as it involves making the 'dirty' money as hard to trace as possible.

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 example, false invoices for goods exported, domestic loan against a foreign deposit, purchasing of property and commingling 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 in and out of personal and business accounts. The money can lie 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) The Prevention of Money Laundering Act ***(discussed in later part of the chapter)***, CBS software should

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

5.6.3 Cyber Crimes

Cyber Crime 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 are 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 and as banks deal with money and use 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.

5.6.4 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 (digitalization of a physical paper cheque into a substitute electronic form for transmission to the paying bank) 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 2000, 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 1st April, 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 Board for Financial Supervision (BFS) is to undertake consolidated supervision of the financial sector comprising commercial banks, financial institution and non-banking finance companies. Some of the key functions of RBI are discussed below:

- **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/destroys currency and coins not 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), 2002

Only relevant sections pertaining to the topic are discussed below:

CHAPTER II OFFENCE OF MONEY-LAUNDERING

Section 3. Offence of money-laundering

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 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 is 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).

Section 70. Offences by companies

(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.

Explanation 1 - 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.

Explanation 2 - 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.

IV. Information Technology Act, 2000

The Information Technology Act (ITA) 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.

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.
- Section 43A: Compensation for failure to protect data.
- Section 65: Tampering with Computer Source Documents.
- Section 66: Computer Related Offences.
- Section 66B: Punishment for dishonestly receiving stolen computer resource or communication device.
- Section 66C: Punishment for identity theft.
- Section 66D: Punishment for cheating by personation by using computer resource.
- Section 66E: Punishment for violation of privacy.

(These sections are already defined in Chapter 1 of the study material.)

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.

(The detail of this concept has been discussed in Chapter 1 of the study material.)

C. Privacy Policy

Every bank 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.

Example 5.7: When a 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 must be informed and provided to user.

The personal information provided by customer such as name, address, phone number, and email are 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.

ILLUSTRATION 5.1

Mr. Shoren has recently been associated with the procurement and sale of drugs and narcotic substances without a license which is illegal as per Narcotic Drugs and Psychotropic Substances Act, 1985. A major part of the sale proceeds amounting to ₹ 65 lakhs was collected and routed through various bank accounts held in SNFC Bank which was subsequently advanced to various bogus companies and a series of transactions were initiated to make the money appear to have been obtained from a legal legitimate source. These activities were carried out with the assistance of one of the employee Mr. Sushil of SNFC Bank who intentionally altered few computer sources codes so that no records for major transactions that took place could be found in the database. A series of transactions ranging from ₹ 10,000 to ₹ 1 lakh was initiated in a month for depositing the amount of ₹ 65 lakhs in SNFC Bank.

However, SNCF Bank had failed to keep proper record of information relating to few of the transactions as they were not of substantial amount. Furthermore, it was later found that one of the staff members of SNFC bank whose relative was an insurance agent, used to obtain medical information of the customers having account with the bank for obtaining personal benefits.

Answer the following Questions:

1. Which amongst the following activities carried out by Mr. Shoren could be considered as an offence of Money Laundering?

   (a) Expenses incurred for procurement of narcotic drugs

(b) Sale of narcotic drugs without a license.

(c) Routing the illegal proceeds through bank and other transactions to appear as obtained from legitimate source.

(d) Being a part of the cartel/association carrying out illegal sale of drugs.

2. An employee of SNFC Bank Mr. Sushil had assisted Mr. Shoren in routing the illegal money through bank by altering the computer source code so that major transactions' amounts were not traceable in the bank's database. Under which Section of IT Act, 2000 will this act of Mr. Sushil is punishable?

(a) Section 66E

(b) Section 66B

(c) Section 65

(d) Section 66D

3. Mr. Shoren was involved in the collection and sale of illegal drugs and got the routing done through various banking transactions and advances to bogus companies. Which stages of Money Laundering process address these aforesaid activities?

(a) Placement and Integration

(b) Layering and Integration

(c) Placement and Layering

(d) Placement, Layering and Integration

4. SNFC Bank failed to maintain records of information relating to baking transactions carried out by Mr. Shoren as many of the transaction amounts were not substantial. Also, the privacy regarding the details of medical history of its customers was breached. Which kind of risk would SNFC bank be exposed to if it has to face legal penalties as it had failed to act in accordance with laws and requirements as per Prevention of Money Laundering Act (PMLA)?

(a) Legal and Compliance Risk

(b) Compliance and Information Security Risk

(c) Information Security and People Risk

(d) Transaction processing and Legal risk

SOLUTION

Question No.	Answer	Question No.	Answer
1.	(c) Routing the illegal proceeds through bank and other transactions to appear as obtained from legitimate source.	**2.**	(c) Section 65
3.	(c) Placement and Layering	**4.**	(b) Compliance and Information Security Risk

ILLUSTRATION 5.2

GNI Bank is one of the age-old conventional banks which offers an array of banking services like EFT'S, Collections, clearing, Letter of credits/guarantees etc. to its customers. To provide latest functionalities and to improve the overall efficiency with respect to banking services, it has recently implemented a core banking solution. It has also put in place the necessary controls to safeguard its business from being exposed to probable IT risks.

Mr. Doshi, a senior software developer having a savings bank account with GNI Bank has requested for internet banking facilities. He has also applied and produced all the necessary documents for availing a housing loan from the said bank. Though the procedures followed for sanctioning housing loans are quite stringent, GNI bank offers floating interest rate on its loans and offers comparatively higher interest rates on its fixed deposits compared to the other banks in the state also.

Answer the following Questions:

1. Given below are the features of Core Banking Solution recently implemented by GNI Bank that prove advantageous to both the bank and its customers. Which among the following advantages would relate the most to Mr. Doshi who has recently availed a housing loan in terms of easy and effortless Internet banking?

   (a) Reliance on transaction balancing

   (b) Highly dependent system-based controls

   (c) Daily, half yearly and annual closing

(d) Automatic processing of standing instructions

2. GNI Bank during this stage of the loan processing of Mr. Doshi, checks the borrower's ability to repay the loan based on an analysis of his credit history, and his earning capacity. This process which forms a major aspect in loan approvals is referred to as _____.

   (a) Clearing

   (b) Underwriting

   (c) Collections

   (d) Letter of Credit

3. GNI bank has also implemented necessary controls to ensure safeguards against the exposure to IT risks. As a practice, whenever a connection is made to website in another network, it will be routed through a particular server. Which among the servers would be utilized for making connections with other network services?

   (a) Web Server

   (b) Application Server

   (c) Proxy Server

   (d) Database Server

4. GSI Bank has also implemented necessary controls to ensure safeguards against the exposure to IT risks. Which among the following controls could be implemented when risk arises due to lack or inadequate management direction and commitment to protect information assets?

   (a) The identity of users is authenticated to the systems through passwords.

   (b) Security policies are established and management monitors compliance with policies.

   (c) Access to sensitive data is logged and the logs are regularly reviewed by management.

   (d) Physical access restrictions are implemented and administered.

SOLUTION

Question No.	Answer	Question No.	Answer
1.	(d) Automatic processing of standing instructions	**2.**	(b) Underwriting
3.	(c) Proxy Server	**4.**	(b) Security policies are established and management monitors compliance with policies.

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, workflow, 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 5.2.1)

2. Enlist the core features of Core Banking Software. **(Refer Section 5.1.4)**

3. Briefly explain major technology components of a CBS solution.

(Refer Section 5.2.2)

4. Discuss various risks that are associated with CBS software.

(Refer Section 5.3.1)

5. List the key provisions of Information Technology Act, 2000 regarding IT related offences impacting banks. **(Refer Section 5.6.4 [Point No. IV])**

6. In line with the suggestions of RBI, ABC Bank is planning to obtain ISO

27001:2013 certification for its Information Security Management System. As an IS Auditor, you are required to prepare a sample list of Risks w.r.t. Information Security for the bank. **(Refer Table 5.3.1)**

7. 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. Considering the above statement, discuss the Money Laundering process and its different stages. **(Refer Section 5.6.2)**

8. Information Technology (IT) risks can be reduced by implementing the right type and level of control in automated environment that is done by integrated controls into information technology. Being an IT consultant, suggest various steps of IT control to a branch manager of a bank.

(Refer Section 5.3.3[Point No. (b])

9. Briefly explain the following terms:

   (a) Proxy Server **(Refer Section 5.2.1[G])**

   (b) Key functions of RBI **(Refer Section 5.6.4[Point No. II])**

10. Discuss various risks and controls associated with the Current and Savings Account (CASA) process. **(Refer Table 5.4.1)**