Chapter -5

CORE BANKING SYSTEMS

OVERVIEW OF BANKING SERVICES

Today banks provide various banking services to citizens staying even at the remotest locationin India.

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

1. Information Technology (IT)

2. Ushering of reforms by successive governments led to huge growth in India's global business.

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.

Q. Why is it important to have Core Banking Systems?

CORE BANKING SYSTEMS (CBS) helps to meet the requirements of its customers, to be able to meet the global challenges in banking and to enhance its service delivery models allowing banks to scale up operations, better service delivery and improved customer satisfaction thereby improving the overall efficiency and performance ofits operations.

Q. What are the key features of banking services?

The core of banking functions is acceptance of deposits and lending of money. The key features of a banking business are as follows:

- The custody of large volumes of monetary items, including cash and negotiable instruments, whose physical security should be ensured.

- Dealing in large volume of transactions.

- Operating through a wide network of branches and departments, which are geographically dispersed?

- Increased possibility of frauds as hence mandatory for banks to provide multi-point authentication checks and the highest level of information security.

Q. Enumerate the major products and services provided and rendered by commercial banks?

1. **Deposits** involve deposits made by customers in various schemes for pre- defined periods. Commercial banks accept deposits in various forms such as term deposits, savings bank deposits, current account deposits, recurring deposits and various other innovative products.

2. **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, securitization of credit sales, housing loans, educational loans, and car loans, etc.

3. **Remittances** involve transfer of funds from one place to another. Most common modes of remittance of funds are as

follows:

4. **Demand Drafts** are issued by one branch of the Bank and are payable by another branch of the Bank The demand drafts are handed over to the applicant.

5. **Mail Transfer (MT)**, no instrument 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.

6. **Electronic Funds Transfer (EFT)** is another mode of remittance which facilitates almost instantaneous transfer of funds between two centers electronically.

7. **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.

8. **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.

9. **Immediate Payment Service (IMPS)** is an instant payment inter-bank electronic funds transfer system in India. IMPS offer 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.

10. **Collections** involve collecting proceeds on behalf of the customer.

11. **Clearing** involves collecting instruments on behalf of customers of bank. The instruments mentioned above may be payable locally or at an outside center. 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

Other Banking Services

a) **Back operations:** These cover all operations done at the back office of the bank. These are related to general ledger, ManagementInformation Systems, reporting, etc.

b) **Retail Banking:** These are also called front-office operations that cover all operations which provide direct retail services to customers for personal use. Eg debit cards, personal loans, mortgages etc.

c) **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.

d) **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

Q. What is meant by CBS and what are its characteristics?

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. Eg Finacle, Flex cube , FinnOne

The characteristics of CBS are as follows:

- There is a common database in a central server located at a Data Center, which gives a consolidated view of the bank's operations.
- Branches function as delivery channels providing services to its customers.
- CBS is centralized Banking Application software that has several components which have been designed to meet the demands of the banking industry.
- CBS is supported by advanced technology infrastructure and has high standards of business functionality.
- Core Banking Solution brings significant benefits such as a customer is a customer of the bank and not only of the branch.
- CBS is modular in structure and is capable of being implemented in stagesas per requirements of the bank.
- A CBS software also enables integration of all third-party applications including in-house banking software to facilitate simple and complex business processes.

Q. What are the key aspects of CBS ?

KEY ASPECTS
- INFORMATION FLOW
- CUSTOMER CENTRIC
- REGULATORY COMPLIANCE
- RESOURCE OPTIMIZATION
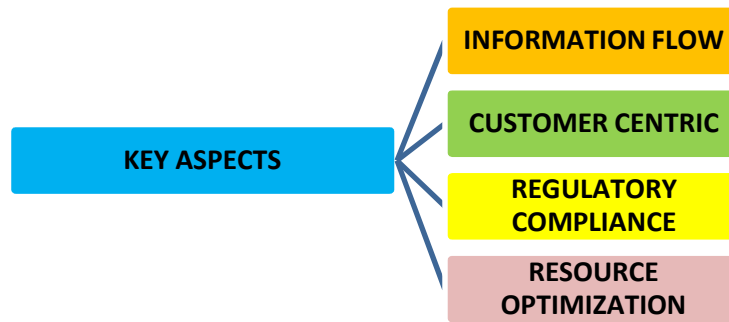
Q. Enumerate the key features of Core Banking Systems .

1) On-line real-time processing.

2) Transactions are posted immediately.

3) All databases updated simultaneously.

4) Centralized Operations (All transactions are stored in one common database/server).

5) Real time seamless merging of data from the back office and self-service operations.

6) Significant reduction in the errors which occurred due to duplication of entries.

7) Separate hierarchy for business and operations.

8) Business and Services are productized.

9) Remote interaction with customers.

10) Reliance on transaction balancing.

11) Highly dependent system-based controls.

12) Authorizations occur within the application.

13) Increased access by staff at various levels based on authorization.

14) Daily, half yearly and annual closing.

15) Lesser operational cost due to less manpower usage.

16) Automatic processing of standing instructions.

17) Centralized interest applications for all accounts and account types.

18) Anytime, anywhere access to customers and vendors.

19) Banking access through multiple channels like mobile, web etc.

Q. Enumerate on the key modules of CBS?

In the case of a CBS, at the core is Central server. All key modules of banking such as back office, branch, data warehouse, ATM Switch, mobile banking, internet banking, phone banking and credit-card system are all connected and related transactions are interfaced with the central server.

Q. Explain the key technology components of CBS ?

1) **Database Environment:** This consists of the centrally located database servers that store the data for all the branches of the bank .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.

2) **Application environment**: It consist of the application servers that host the different core banking systems like Flex Cube, Bank Mate etc. and is centrally used by different banks. The access to these application servers will generally be routed through a firewall.

3) **Enterprise Security Architecture & Security Solution:** To ensure security; proxy servers, firewalls, intrusion detection systems are used to protect the network from any malicious attacks and to detect any unauthorized network entries. Periodic assessment and testing are carried out to assess the vulnerability and identify the weaknesses.

4) **Connectivity to the Corporate Network and the Internet:** Network administration also plays a very significant role in core banking systems. There should be adequate bandwidth to deal with the volume of transactions so as to prevent slowing down and resulting in lower efficiency.

5) **Data Centre and Disaster Recovery Centre:** The core banking systems consists 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.

6) **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. 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.

Q. Enumerate the different steps in the implementation of CBS ?

1) **Planning: D**one as per strategic and business objectives of bank.

2) **Approval:** The decision to implement CBS should be approved by the board of directors as it requires high investment and recurring costs

3) **Selection:** Select the right solution by the bank to meet their specific requirements and business objectives.

4) **Design and develop or procured:** Appropriate controls covering the design or development or procurement of CBS for the bank.

5) **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.

6) **Implementation:** CBS must be implemented as per pre-defined and agreed plan with specific project milestones to ensure successful implementation.

7) **Maintenance:** CBS must be maintained as required. E.g. program bugs fixed, version changes implemented, etc.

8) **Support:** CBS must be supported to ensure that it is working effectively.

9) **Updation:** CBS modules must be updated based on requirements of business processes, technology updates and regulatory requirements;

10) **Audit:** Audit of CBS must be done internally and externally as required to ensure that controls are working as envisaged.

Q. List down the components of CBS IT Environment.

1) Application Server
2) Database Server
3) ATM Channel Server
4) Internet Banking Channel server
5) Internet Banking Application Server
6) Web Server
7) Proxy Server
8) Anti virus software server

Q. What are the core business process in CBS?

1) Current and Savings account
2) Credit Cards
3) Loans and Trade Finance
4) Mortgage /Property Loans
5) Internet banking process
6) Treasury process

Q. Enumerate the different sub processes involved in Information Security?

- **Information Security Policies, Procedures and practices:** This refers to the processes relating to approval and implementation of information 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.

- **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.

- **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.

Q. What are the risks and controls associated with Information security in banks?

Risk	Controls
Significant information resources may be modified inappropriately, disclosed without authorization, and/or unavailable when needed.	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.	The password is periodically changed, kept confidential and complex (e.g., password length, alphanumeric content, etc.).
Unauthorized viewing, modification or copying of data and/ or unauthorized use, modification or denial of service in the system.	System owners authorize the nature and extent of user access privileges, and such privileges are periodically reviewed bysystem owners.
Security breaches may go undetected.	Access to sensitive data is logged and the logs are regularly reviewed by management.
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.
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

Q. What are the different types of risk associated with the core banking system?

1) **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. The components of operational risk include the following :

a) **Processing Risk** arises because faulty reporting of important market developments to the bank management may also occur due to errors in entry of data for subsequent bank computations.

b) **Information Security Risk** comprises the impacts 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.

c) **Legal Risk** arises because of the treatment of clients, the sale of products, or business practices of a bank.

d) **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.

e) **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.

2) **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.

3) **Market Risk:** Market risk refers to the risk of losses in the bank's tradingbook 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.

4) **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.

5) **IT Risk:**. Some of the common IT risks related to CBS are as follows:

a) Ownership of Data/ process

b) Authorization process

c) Authentication procedures

d) Several software interfaces across diverse networks

e) Maintaining response time

f) User Identity Management

g) Access Controls

h) Incident handling procedures

i) Change Management

Q. What are the risk and controls in CASA Process?

	Risk in CASA	Key Controls
1.	Credit Line setup is unauthorized and not in line with the bank's policy.	The credit committee checks that the Financial Ratios, the Net-worth, the Risk factors and its corresponding mitigating factors, the Credit Line offered and the Credit amount etc. is in line with Credit Risk Policy and that the Client can be given the Credit Line.
2.	Credit Line setup in CBS is unauthorized and not in line with the bank's policy.	Access rights to authorize the credit limit in case of account setup system should be restricted to authorized personnel.
3.	Customer Master defined in CBS is not in accordance with the Pre- Disbursement Certificate.	Access rights to authorize the customer master in CBS should be restricted to authorized personnel.
4.	Inaccurate interest / charge being calculated in CBS.	Interest on fund based facilities is automatically calculated in the CBS as per the defined rules.
5.	Unauthorized personnel approving the CASAS transaction in CBS.	Segregation of Duties to be maintained between the initiator and authorizer of the transaction for processing transaction in CBS.

Q. What are the risks and controls with respect to credit cards?

Risk wrt to credit cards	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 CASAS transaction in CBS.	Segregation of Duties to be maintained between the initiator and authorizer of the transaction for processing transaction in CBS.
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.

Q. What are the risks and controls with respect to mortgages?

Risk wrt to mortgages	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 incorrectly 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.*

Q. What are the risks and control with respect to treasury process?

Risk wrt to treasury	Key Controls
Unauthorized securities setup in systems such as Front office/Back office.	Appropriate Segregation of duties and review controls around securities master setup/ amendments.
Inaccurate trade is processed.	Appropriate Segregation of duties 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 CCIL/NEFT/RTGS settlements to ensure the margin funds availability and the timely funds settlements.
Incorrect Nostro payments processed.	Controls at Nostro reconciliation and payments.

Q. What are the risks and controls associated with loans and advances?

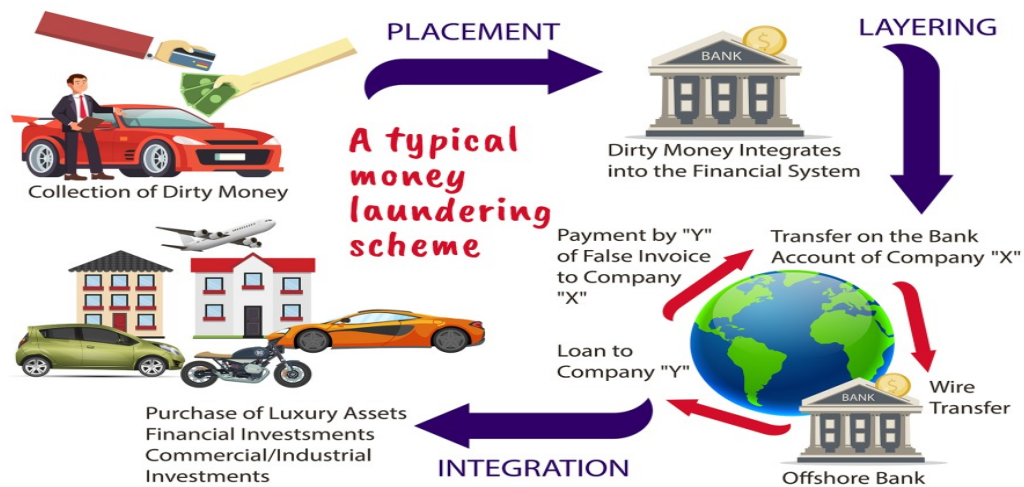| Risk	Key Controls
Credit Line setup is unauthorized and not in line with the bank's policy.	*The credit committee checks that the Financial Ratios, the Net-worth, the Risk factors and its corresponding mitigating factors, the Credit Line offered and the Credit amount etc. is in line with Credit Risk 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	*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*
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.*

Q. Enumerate the functions of RBI?

a) Regulation and supervision of banks.

b) Formulates implements and monitors the monitory policy.

c) Issuance and regulation of currency.

d) Inspection of banks.

Q. What is meant by money laundering and what are the different stages involved in money laundering?

- Money Laundering is the process by which the proceeds of the crime and the true ownership of those proceeds are concealed or made opaque so that the proceeds appear to come from a legitimate source.

- The objective in money laundering is to conceal the existence, illegal source, or illegal application of income to make it appear legitimate.

- Money laundering is commonly used by criminals to make 'dirty' money appear 'clean'

The different stages involved in money laundering are

1) Placement

2) Layering

3) Integration

A typical money laundering scheme

PLACEMENT — Collection of Dirty Money → Dirty Money Integrates into the Financial System

LAYERING — Transfer on the Bank Account of Company "X" → Wire Transfer → Offshore Bank → Loan to Company "Y" → Payment by "Y" of False Invoice to Company "X"

INTEGRATION — Purchase of Luxury Assets, Financial Investments, Commercial/Industrial Investments

Q. Explain the different stages in money laundering?

a) PLACEMENT - The first stage movement of proceeds from the scene of the crime to a place, or into a form, less suspicious and more convenient for the criminal.

b) LAYERING - It involves separation of proceeds by sending the money through various complex financial transactions to change its form and make it difficult to follow and hide the proceeds.

c) INTEGRATION - It involves conversion of illegal proceeds into apparently legitimate business earnings through normal financial or commercial operations.

Q. Enumerate the different reporting requirements of entities as per Section 12 of PMLA ?

Every reporting entity(banking companies, financial institutions and intermediaries) shall maintain a record of all transactions

a) 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;

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

Q. What is meant by cyber crimes and what does it constitute?

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.

a) Committing of a fraud by manipulation of the input, output, or throughput of acomputer-based system.

b) Computer forgery, which involves changing images or data stored incomputers,

c) Deliberate damage caused to computer data or programs through virusprograms or logic bombs,

d) Unauthorized access to computers by 'hacking' into systems or stealingpasswords, and,

e) Unauthorized reproduction of computer programs or software piracy.

f) Cybercrimes have grown big with some countries promoting it to attackanother country's security and financial health.

Q. List down the key provisions of Information Technology Act 2008 ?

Section 43: Penalty and compensation for damage to computer, computer system

Section 65: Tampering with Computer Source Documents

Section 66: Computer Related Offences

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

Section 66-C: Punishment for identity theft

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

Section 66-E: Punishment for violation of privacy

Q. What constitutes Sensitive personal data?

Sensitive Personal Data or Information', 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.