After reading this chapter, you will be able to -

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

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

☑ Comprehend regulatory and compliance requirements applicable to CBS such as Banking Regulations Act, RBI regulations, Prevention of Money Laundering Act and Information Technology Act.
5.1 OVERVIEW OF BANKING SERVICES AND RELATED IT RISK AND CONTROLS

5.1.1 INTRODUCTION

Information Technology (IT) is an integral aspect of functioning of enterprises and professionals in this digital age. In case of banking which deals with money, has now increasingly become digital and IT plays a very critical role. The rapid strides in IT and its rapid adoption by banks in India have empowered banks to use IT extensively to offer...
newer products and services to customers apart from automating internal processes and information systems. The dependence on IT is such that the banking business cannot be thought of in isolation without IT. There has been massive use of technology across many areas of banking business in India, both from the asset and the liability side of a bank’s balance sheet. The technology footprint has spread across the Indian banking landscape in a very big way. In fact, with most banks using technology, the key differentiator now is how IT is used for delivering services to customers. Delivery channels have immensely increased the choices offered to the customer to conduct transactions with ease and convenience. Various wholesale and retail payment and settlement systems have enabled faster means of moving the money to settle funds among banks and customers, facilitating higher turnover of all financial transactions using IT. Developments in IT have also ushered in a whole set of challenges, issues and risks to deal with as most of the data is automated and thus available in digital form.

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

5.1.2 Overview of Banking Services

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

- The custody of large volumes of monetary items, including cash and negotiable instruments, whose physical security should be ensured.
- Dealing in large volume (in number, value and variety) of transactions.
- Operating through a wide network of branches and departments, which are geographically dispersed.
- Increased possibility of frauds as banks directly deal with money making it mandatory for banks to provide multi-point authentication checks and the
There are various types of banks providing specific range of banking services. Hence, it is not necessary that all banks provide all type of services. However, core banking services relating to deposit, advances and services are provided by most of the banks. To understand how automation impacts the way these services are provided, it is critical to understand various types of banking services and how these services are provided. Some of the major products and services provided and rendered by commercial banks which constitute core banking services are briefly explained here.

I. Acceptance of Deposits

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

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.

III. Remittances

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

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 drawer of the bill). They can also lodge their term deposit receipts and other similar instruments with the Bank for collection of the proceeds from the Bank with which the term deposit, etc. is maintained. Banks also collect instruments issued by post offices, like national savings certificates, postal orders, etc.

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 to the branches of the issuing Bank at those centers or, if there is no such branch, to other banks. Clearing house settles the inter-Bank transactions among the local participating member banks. Generally, post offices are also members of the house. There may be separate clearing houses for MICR (Magnetic Ink Character Recognition) and non-MICR instruments. MICR is a technology which allows machines to read and process cheques enabling thousands of cheque transactions in a short time. MICR code is usually a nine-digit code comprising of some important information about the transaction and the bank.

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

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

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

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

© The Institute of Chartered Accountants of India
VI. Letters of Credit and Guarantees

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

VII. Credit Cards

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

VIII. Debit Cards

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

IX. Other Banking Services

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

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

- **Retail Banking**: These are also called front-office operations that cover all operations which provide direct retail services to customers.

- **High Net-worth Individuals (HNI)**: Banks provide special services to...
customers classified as High Net-worth Individuals (HNI) based on value/volume of deposits/transactions.

**Fig. 5.1.1: Banking Services**

- **Risk Management**: Risks are all pervasive in the banking sector. This should be done at strategic, tactical, operational and technology areas of the bank. Risk management is best driven as per policy with detailed standards, procedures and guidelines provided for uniform implementation.

- **Specialized Services**: Banks also perform other services such as insurance broking, claims, underwriting, life insurance, non-life insurance, etc. However, these would be offered by separate entities set up by the bank.

**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. These are not explained here as these are not core banking activities. All bank may not carry all given services. Some services such as insurance, underwriting, etc. may be done through separate subsidiaries.

**5.1.3 Challenges of IT**

The dependence on technology in banking for most of the key banking services and processes has led to various challenges. IT risks are also taking new forms and transforming as well. The business processes and standards adapted by Banks should consider these new set of IT risks and challenges:

(i) **Frequent changes or obsolescence of technology**: Technology keeps on evolving and changing constantly and becomes obsolete very quickly. Hence, there is always a risk that the investment in technology solutions unless properly planned may result in loss to bank due to risk of obsolescence.

(ii) **Multiplicity and complexity of systems**: The core of banking services remain
same but by using technology the way these banking products and services are provided changes drastically. The Technology architecture used for services could include multiple digital platforms and is quite complex. Hence, this requires the bank personnel to have personnel with requisite technology skills or the management of the bank’s technology could be outsourced to a company having the relevant skill set.

(iii) **Different types of controls for different types of technologies/ systems:** Deployment of Technology gives rise to new types of risks which are explained later in this chapter. These risks need to be mitigated by relevant controls as applicable to the technology/information systems deployed in the bank.

(iv) **Proper alignment with business objectives and legal/ regulatory requirements:** Banks must ensure that the CBS and allied systems implemented, cater to all the business objectives and needs of the bank, in addition to the legal/regulatory requirements envisaged.

(v) **Dependence on vendors due to outsourcing of IT services:** In a CBS environment, the bank requires staff with specialized domain skills to manage IT deployed by the bank. Hence, these services could be outsourced to vendors and there is heavy dependency on vendors and gives rise to vendor risks which should be managed by proper contracts, controls and monitoring.

(vi) **Vendor related concentration risk:** There may not be one but multiple vendors providing different services. For example, network, hardware, system software and banking software services may be provided by different vendors or these services may be provided by a single vendor. Both these situations result in higher risks due to heavy dependence on vendors.

(vii) **Segregation of Duties (SoD):** Banks have a highly-defined organization structure with clearly defined roles, authority and responsibility. The segregation of duties as per organization structure should be clearly mapped in the CBS used by the bank. This is a high-risk area since any SoD conflicts can be a potential vulnerability for fraudulent activities. For example, if a single employee can initiate, authorize and disburse a loan the possibility of misuse cannot be ignored.

(viii) **External threats leading to cyber frauds/ crime:** The CBS environment provides access to customers anytime, anywhere using internet. Hence, information system which was earlier accessible only within and to the employees of the bank is now exposed as it is open to be accessed by anyone from anywhere. Making the information available is business imperative but this is also fraught with risks of increased threats from hackers and others who could access the software to commit frauds/crime.

(ix) **Higher impact due to intentional or unintentional acts of internal employees:** Employees in a technology environment are the weakest link in an enterprise.
This is much more relevant in bank as banks deal directly with money. Hence, the employee acts done intentionally or unintentionally may compromise security of the IT environment.

(x) **New social engineering techniques employed to acquire confidential credentials:** Fraudsters use new social engineering techniques such as socializing with employees and extracting information which is used unauthorizedly to commit frauds. For example: extracting information about passwords from bank’s staff acting as genuine customer and using it to commit frauds.

(xi) **Need for governance processes to adequately manage technology and information security:** Controls in CBS should be implemented from macro and business perspective and not just from function and technology perspective. As Technology, has become key enabler for bank and is implemented across the bank, senior management of bank should be involved in directing how technology is deployed in bank and approve appropriate policies. This requires governance process to implement security as required.

(xii) **Need to ensure continuity of business processes in the event of major exigencies:** The high dependence on technology makes it imperative to ensure resilience to ensure that failure does not impact banking services. Hence, a documented business continuity plan with adequate technology and information systems should be planned, implemented and monitored.

### 5.1.4 IT Risks and Risk Assessment

Every enterprise is started and exists to provide value to its stakeholders. Value could be in terms of profit or growth for investors or services rendered for non-profit or government entities. Banks, whether public or private strive to provide value to various stakeholders. Every business has its own inherent risk and banking business is prone to higher risk. Similarly, automation of business processes introduces new types of risks and in case of banking services, as it primarily involves with money, there are greater and newer risks. So, it should be quite clear that automated banking has higher risks and these risks need to be understood and mitigated by appropriate risk mitigation strategies.

I. **Definition of Risk**

There are multiple definitions of Risk.

- As per International Organization for Standardization (ISO): Risk is uncertainty in achieving objectives. Risk can be positive or negative.

- In simple terms, Risk can be defined as: “the potential harm caused if a threat exploits a particular vulnerability to cause damage to an asset”. For example: inadequate security is a vulnerability which could be exploited by a hacker.
• **Risk Analysis** is defined as the process of identifying security risks and determining their magnitude and impact on an organization. Information systems can generate many direct and indirect risks. These risks lead to a gap between the need to protect systems and the degree of protection applied. The gap is caused by:
  o Widespread use of technology and Interconnectivity of systems;
  o Elimination of distance, time and space as constraints;
  o Devolution of management and control;
  o Attractiveness of conducting unconventional digital attacks; and
  o External factors such as legislative, legal and regulatory requirements or IT developments.

• Risks are mitigated by implementing risk assessment. This involves the following:
  o Identification of threats and vulnerabilities in the system;
  o Potential impact or magnitude of harm that a loss of security would have on enterprise operations or enterprise assets, should an identified vulnerability be exploited by a threat; and
  o The identification and analysis of security controls for information systems.

II. **Impact of IT Risks**

IT risks not only have a direct impact on banks as operational risks but can also exacerbate other risks like credit risks and market risks. Given the increasing reliance of customers on digital delivery channels to conduct transactions, any security related issues have the potential to undermine public confidence in the use of online banking channels and lead to reputation risks to the banks. Inadequate and improper IT implementation can also induce strategic risk in terms of strategic decision making based on inaccurate data/information. Compliance risk is also an outcome in the event of non-adherence to regulatory or legal requirements arising out of the use of IT. These issues ultimately have the potential to impact the safety and soundness of a bank and in extreme cases may lead to systemic crisis. There are new IT risks which could have a significant impact on critical business operations, such as:

(i) External dangers from hackers, leading to denial of service and virus attacks, extortion and leakage of corporate information.

(ii) Growing potential for misuse and abuse of information system affecting privacy and ethical values; and Increasing requirements for availability and robustness.

(iii) Phishing attacks through Internet Banking. Phishing is the attempt to
obtain sensitive information such as usernames, passwords, and credit card
details (and, indirectly, money), often for malicious reasons, by disguising
as a trustworthy entity in an electronic communication.

III. IT Risk Management

Effective risk management begins with a clear understanding of the bank’s risk
appetite and identifying high-level risk exposures. After defining risk appetite
and identified risk exposure, strategies for managing risk can be set and
responsibilities clarified. Based on the type of risk, project and its significance to
the business, Board and Senior Management may choose to take up any of the
following risk management strategy in isolation or combination as required:

- **Avoid**: Eliminate the risk by not taking up or avoiding the specific business
  process which involves risk.
- **Mitigate**: Implement controls (e.g. acquire and deploy security technology
to protect the IT infrastructure).
- **Transfer**: Share risk with partners or transfer to insurance coverage.
- **Accept**: Formally acknowledge that the risk exists and monitor it.

Some sample risks relating to Banking are as follows:

- Loss of confidential data;
- Unauthorized access to customer information;
- Inaccuracy of data leading to incorrect decision-making;
- Loss due to errors;
- Loss of money/reputation/business due to Frauds; and
- Impact of Non-compliance.

IV. Examples of IT Risk Assessment and Risk Management Mechanism

Automation makes each of the banking areas prone to different types of risks. Some
examples of risks are as follows:

**a. Risks to Data**

- Unauthorized data changes affecting integrity of data;
- Absence of logs and audit trail/ logs;
- Unauthorized transactions;
- Unauthorized entry/ corrections/ deletions;
- Transactions without vouchers;
- Changing data using other’s password;
Willful and wrong inputs; and
Hiding erroneous outputs

b. Other IT Risks
- Unauthorized or incorrect Interest rate changes;
- Incorrect Interest computation;
- Incorrect computation of charges;
- Unauthorized increased in credit limits;
- Payments of stolen drafts;
- Payment of stopped cheques;
- Payment of duplicate drafts/ Fixed Deposit Certificates issued; and
- Opening of New accounts without complying with KYC (Know Your Customer) norms as specified by RBI.

V. Indicators of higher IT risk
The review of risk assessment and risk management should be done on regular basis as risks are dynamic and keep on changing. Some of the risk indicators are:

- IT security is not given required priority;
- Attitude of "Computer will take care of everything – no checking is required";
- Lack of transparency of IT operations and responsibility assigned;
- Lack of Input control;
- Lack of output verification;
- Lack of evidence;
- Lack of access control;
- Lack of audit trails;
- Lack of dual checks for sensitive and high value transactions;
- Lack of documented disaster recovery plan/ contingency plan/ Business Continuity Plan;
- Lack of controls leading to temptation to commit frauds;
- No check on vendors for reliability of software; and
- Over-dependence on long serving – ‘trusted’ operators, supervisors, managers, etc.

© The Institute of Chartered Accountants of India
VI. Importance of IT Controls

Control refers to the policies, procedures, practices and organization structures that are designed to provide reasonable assurance that business objectives are achieved and undesired events are prevented or detected and corrected. IT Controls are implemented to achieve control objectives and are implemented through specific set of control procedures. IT Control objectives is defined as: “a statement of the desired result or purpose to be achieved by implementing control procedures within a particular IT activity”. Implementing right type of controls is responsibility of management. Controls provides a clear policy and good practice for directing and monitoring performance of IT to achieve enterprise objectives. IT Controls perform dual role:

(i) They enable enterprise to achieve objectives; and
(ii) They help in mitigating risks.

Many issues drive the need for implementing IT controls. These range from the need to control costs and remain competitive to the need for compliance with internal and external governance. IT controls promote reliability and efficiency and allow the organization to adapt to changing risk environments. Any control that mitigates or detects fraud or cyber-attacks enhances the organization’s resiliency because it helps the organization uncover the risk and manage its impact. Resiliency is a result of a strong system of internal controls which enable a well-controlled organization-to manage challenges or disruptions seamlessly.

VII. Key indicators of effective IT controls

- The ability to execute and plan new work such as IT infrastructure upgrades required to support new products and services.
- Development projects that are delivered on time and within budget, resulting in cost-effective and better product and service offerings compared to competitors.
- Ability to allocate resources predictably.
- Consistent availability and reliability of information and IT services across the organisation and for customers, business partners, and other external interfaces.
- Clear communication to management of key indicators of effective controls.
- The ability to protect against new vulnerabilities and threats and to recover from any disruption of IT services quickly and efficiently.
- The efficient use of a customer support center or help desk.
VIII. Internal Control System in Banks

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

(a) Internal Controls in Banks

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

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

(b) IT Controls in Banks

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

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

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

5.1.5 Applying IT Controls

The risks and controls explained earlier in the section should be implemented within IT. Hence, it is important for the bank to identify controls as per policy, procedures and organization structure of the bank and configure it within IT software as used in the bank. There are different options for implementing controls as per risk management strategy. For example, the way banking is done in nationalized bank is traditional way with rigid organization structure of managers at different levels, officers and clerks and clear demarcation between departments and functions whereas in a private sector, the organization structure is organized around customers and focused on relationship banking. Each of these IT deployments of CBS requires applying IT controls as per specific requirements of the bank. This application of controls is done through proper configuration settings, setting of parameters in masters and implementing controls in transaction processing.

IT controls are selected and implemented based on the risks they are designed to manage. As risks are identified, suitable risk responses are determined, ranging from doing nothing and accepting the risk as a cost of doing business to applying a wide range of specific controls, including insurance. Controls always involve costs. Hence, it is important to ensure that adequate and appropriate controls are implemented to mitigate the risks as applicable. In case of banking industry, risks are all pervasive.
However, the focus in this chapter is not on business related risks of banking but IT related risks and controls of banking automation.

Apart from the classification of controls already discussed in detail in previous chapter, a common classification of IT controls is **General Controls** and **Application Controls**. General Controls are macro in nature and the impact pervades the IT environment at different layers whereas Application Controls are controls which are specific to the application software.

(a) **General Controls**

**General Controls**, also known as Infrastructure Controls pervade across different layers of IT environment and information systems. General Controls are pervasive controls and apply to all systems components, processes, and data for a given enterprise or systems environment. General controls include, but are not limited to:

- **Information Security Policy**: The security policy is approved by the senior management and encompasses all areas of operations of bank and drives access to information across the enterprise and other stakeholders.

- **Administration, Access, and Authentication**: IT should be administered with appropriate policies and procedures clearly defining the levels of access to information and authentication of users.

- **Separation of key IT functions**: Secure deployment of IT requires the bank to have separate IT organisation structure with key demarcation of duties for different personnel within IT department and to ensure that there are no SoD conflicts.

- **Management of Systems Acquisition and Implementation**: Software solutions for CBS are most developed acquired and implemented. Hence, process of acquisition and implementation of systems should be properly controlled.

- **Change Management**: IT solutions deployed and its various components must be changed in tune with changing needs as per changes in technology environment, business processes, regulatory and compliance requirements. These changes impact the live environment of banking services. Hence, change management process should be implemented to ensure smooth transition to new environments covering all key changes including hardware, software and business processes. All changes must be properly approved by the management, before implementation.

- **Backup, Recovery and Business Continuity**: Heavy dependence on IT and criticality makes it imperative that resilience of banking operations should be ensured by having appropriate business continuity including backup, recovery and off-site data centre.
Proper Development and Implementation of Application Software: Application software drives the business processes of the banks. These solutions in case developed and implemented must be properly controlled by using standard software development process.

Confidentiality, Integrity and Availability of Software and data files: Security is implemented to ensure Confidentiality, Integrity and Availability (CIA) of information. **Confidentiality** refers to protection of critical information. **Integrity** refers to ensuring authenticity of information at all stages of processing. **Availability** refers to ensuring availability of information to users when required. IT operations refer to how IT is deployed, implemented and maintained within the bank. All IT operations need to be controlled by appropriate policies and procedures.

Incident response and management: There may be various incidents created due to failure of IT. These incidents need to be appropriately responded and managed as per pre-defined policies and procedures.

It is important to note that proper and consistent operation of automated controls or IT functionality often depends upon effective IT general controls. In later sections, detailed risk and control matrix for various types of general controls are provided.

(b) **Application Controls**

**Application Controls** are controls which are implemented in an application to prevent or detect and correct errors. These controls are in-built in the application software to ensure accurate and reliable processing. Application controls ensure that all transactions are authorized, complete and accurate. Application Controls pertain to the scope of individual business processes or application systems. For example: application software ensures that only transactions of the day are accepted by the system. Withdrawals are not allowed beyond limits, etc. Some examples of Application controls are as follows:

- Data edits (editing of data is allowed only for permissible fields);
- Separation of business functions (e.g., transaction initiation versus authorization);
- Balancing of processing totals (debit and credit of all transactions are tallied);
- Transaction logging (all transactions are identified with unique id and logged);
- Error reporting (errors in processing are reported); and
- Exception Reporting (all exceptions are reported).

A detailed discussion of Application Controls has already been provided in the previous chapter.
5.2 COMPONENT AND ARCHITECTURE OF CBS

5.2.1 Overview of CBS

Core Banking Solution (CBS) refers to a common IT solution wherein a central shared database supports the entire banking application. Business processes in all the branches of a bank update 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. These factors provide banks with a competitive edge. Core Banking Solution brings significant benefits such as a customer is a customer of the bank and not only of the branch. Further, the CBS is modular in structure and is capable of being implemented in stages as per requirements of the bank. A CBS software also enables integration of all third-party applications, including in-house banking software, to facilitate simple and complex business processes. Some examples of CBS software are given below. These are only illustrative and not exhaustive.

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

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

© The Institute of Chartered Accountants of India
Key modules of CBS are given in the Fig. 5.2.1:

![Diagram of Key Modules of CBS](image)

**Fig. 5.2.1: Key Modules of CBS**

Fig. 5.2.1 is a simple diagram illustrating how most of the key modules of bank are connected to a common central server. In the case of a CBS, at the core is Central server. All key modules of banking such as back office, branch, data warehouse, ATM Switch, mobile banking, internet banking, phone banking and credit-card system are all connected and related transactions are interfaced with the central server.

**5.2.2 CBS Architecture**

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

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

© The Institute of Chartered Accountants of India
Banks make these services available across multiple channels like ATMs, Internet banking, and branches.

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

- **Information flow**: Facilitates information flow within the bank and improves the speed and accuracy of decision-making. It deploys systems that streamline integration and unite corporate information to create a comprehensive analytical infrastructure.

- **Customer centric**: Through a holistic core banking architecture, enables banks to target customers with the right offers at the right time with the right channel to increase profitability.

- **Regulatory compliance**: Compliance in case of banks is complex and expensive. CBS has built-in and regularly updated regulatory platform which will ensure compliance.

- **Resource optimization**: 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 Core features of CBS

Initially, basic modules like Savings Account, Current Account, Fixed Deposits, Bills & Remittances, Loans and Advances models were implemented. Subsequently, alternate delivery channels like ATM, Internet banking, Real Time Gross Settlement (RTGS)/National Electronics Funds Transfer System (NEFT), Mobile Banking, Treasury, Government Business etc. could be added. As servers are on 24 hours on all days, banking can be done at any time and from anywhere. Database of customers is updated on-line on a real-time basis. For example, amount withdrawn at any ATM by the customer is deducted from the customer’s balance almost instantly. Similarly, in case of online transaction, for transfer of funds by customer, the transaction is updated instantly in both the banks and respective accounts are updated at all levels.

The core features of CBS are as follows:

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

5.2.4 Major components of the CBS solution

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.

The various components/ features of core banking are as follows:

- Opening new accounts and customer on-boarding.
- Managing deposits and withdrawals.
- Transactions management from initiation to reporting.
- Interest calculation and management.
- Payments processing (cash, cheques/ mandates, NEFT, RTGS, IMPS etc.).
- Loans disbursement and management.
- Processing cash deposits and withdrawals.
- Processing payments and cheques.
- Processing and servicing loans.
- Accounts management.
- Configuring and calculating interest.
- Customer Relationship Management (CRM) activities.
- Setting criteria for minimum balances, interest rates, withdrawals allowed,
5.2.2 ENTERPRISE INFORMATION SYSTEMS

- Maintaining records for all the bank’s transactions.

The branch confines itself to the following key functions:
- Creating manual documents capturing data required for input into software
- Internal authorization
- Initiating Beginning-Of-Day (BOD) operations
- End-Of-Day (EOD) operations
- Reviewing reports for control and error correction.

5.2.5 Technology and work-flow of CBS

CBS involves banking services provided by a group of networked bank branches. As they are networked, customers can access their accounts and perform certain transactions from any of the bank’s branches. The customer is no longer a customer of the branch but is a customer of the bank. CBS is a combination of an application software and network devices. There is a Central Data Centre which is a Data Centre which has a large data housing infrastructure providing high band width access to its clients.

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. CBS has brought significant changes so far as workflow and housekeeping activities/ accounting processes at branches are concerned.

- User-actions and controls are elaborately menu-driven.
- User is prompted by software to initiate an action and to apply a control.
- Various periodical runs/ mass activities like Application of Interest & Service Charges,
- Updating of parameters globally, balancing/ reconciliation of ledgers and TDS etc. are carried out centrally at the Data Centre, leaving various control actions to be taken at branches.

5.2.6 Technology Components

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

The key technology components of CBS are as follows:
- Database Environment

© The Institute of Chartered Accountants of India
1. Technology Architecture of CBS

The Fig. 5.2.2 provides an architecture overview of CBS 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. These concepts are further explained in later section (CBS IT Environment) of this chapter.

**Architecture Overview**

**Client**
- **Teller**: Browser or Client/Server
- **Customer**: branch, ATM, POS, telephone, Internet, TV browser, PDA, mobile phone etc.

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

**Application Servers**
- Business Intelligence
- TP Monitors
- Host Connect

**Host Database Server**
- Oracle RDBMS
- Execution Logic

© The Institute of Chartered Accountants of India
II. 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. 5.2.3 provides a functional architecture of CBS covering the complete range of banking services.

Fig. 5.2.3: Functional Architecture of CBS\(^1\) (Illustrative)

\(^1\) Source: Finacle © The Institute of Chartered Accountants of India
5.2.3 How Does CBS Work?

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

- **Planning:** Planning for implementing the CBS should be done as per strategic and business objectives of bank.

- **Approval:** The decision to implement CBS requires high investment and recurring costs and will impact how banking services are provided by the bank. Hence, the decision must be approved by the board of directors.

- **Selection:** Although there are multiple vendors of CBS, each solution has key differentiators. Hence, bank should select the right solution considering various parameters as defined by the bank to meet their specific requirements and business objectives.

- **Design and Develop/ Procure:** CBS solutions used to be earlier developed in-house by the bank. Currently, most of the CBS deployment are procured. There should be appropriate controls covering the design or development or procurement of CBS for the bank.

- **Testing:** Extensive testing must be done before the CBS is live. The testing is to be done at different phases at procurement stage to test suitability to data migration to ensure all existing data is correctly migrated and testing to confirm processing of various types of transactions of all modules produces the correct results.

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

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

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

- **Updation:** CBS modules must be updated based on requirements of business processes, technology updates and regulatory requirements.
Audit: Audit of CBS must be done internally and externally as required to ensure that controls are working as envisaged.

Fundamentally, in a CBS, all the bank’s branches access applications from centralized data-centers. Core banking systems are akin to a human heart in terms of importance and functionality. All transactions are routed through core systems, which are available 24 x 7 and accessible from anywhere, anytime and through multiple devices such as desktops, laptops, ATM, Internet, mobile phone, tablets, etc.

The following diagram provides an overview of how a CBS works. It may be noted that the core of CBS is the customer who interacts with CBS through various channels such as branches, ATMs, call centres, internet banking, relationship officers of bank or through mobile phones. These delivery channels connect to different business modules/ silos in an integrated manner. These functional modules connect to various types of servers such as database server, CRM server, application server, data warehouse server, ATM servers, etc. In addition, partners/ vendors may also be connected to the CBS.

Customer Identification File (CIF) is a digital or virtual file where the customer identity details with a valid photo ID and address details are stored and given a unique number which is called CIF number. A customer may have many accounts of different nature, like current account, savings account, loans etc., but all these accounts will be mapped to one CIF only.

---

© The Institute of Chartered Accountants of India
5.2.4 CBS IT Environment

The CBS facilities providing banking services for branches of a bank which are networked and connected to common data center. This facilitates staff to process transactions of customers of any branch. Customers can also access their accounts and perform specific transactions as per pre-defined access from any of the bank’s branches or online. Hence, all the customers of all the branches are customers of the bank. Core banking solutions (CBS) is provided through a combination of an application software and network devices. There is a Central Data Centre. The Data Centre is a large data housing infrastructure that provides high bandwidth access to bank and its customers. The core banking environment would comprise of a Central Application Server that runs the Core Banking Solution (CBS) with the application software being centrally accessed by all the branches as also customers.

A. Servers

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. There are different types of servers used in deploying CBS. Some of these are briefly explained here:

(i) Application Server
(ii) Database Server
(iii) Automated Teller Machine channel Server,
(iv) Internet Banking Channel Server,
(v) Internet Banking Application Server
(vi) Web Server,
(vii) Proxy Server,
(viii) Anti-Virus Software Server, etc.

This server is a powerful and robust system as performs the entire core banking operations. CBS is developed as internet based application and therefore can be accessed through browser application. Application server may be decentralized and located at regional office or at branch for easy and quick response. No user is granted access to CBS directly. Access is always through channel server that processes the request and fetches or sends data to CBS for updating. The validation is a complete process in the computer so that it ensures that data that is fed in, conforms to certain prerequisite conditions e.g., if an operator keys in data for withdrawal of money, the account number of customer would be entered by the operator naturally. But there would be a built-in control so that further processing would be entertained only after the systems verifies that the account number which is now entered is already in the database i.e., it is an existing customer. After the data is validated at the branch, it
would be sent to the respective channel server in the centralized data center. The channel (which houses the respective channel software) after receiving data performs necessary operations and updates the core database, etc.

I. Application Server

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

The application software, CBS, which is in the application server is always to be the latest version as accepted after adequate testing; the application software is never static and would require some changes to be effected either due to bugs discovered or a change in the process or any other justified reason. Such changes are never made directly into the live application server. These changes are made to a separate server called a test server. The programs are debugged and certified that the program is now amended as required and performs as expected. The changed and latest application software will be moved into the application server under proper authority. The earlier version would be archived and the latest copy of the software would always have a backup copy.

II. Database Server

The Database Server of the Bank contains the entire data of the Bank. The data would consist of various accounts of the customers and master data (e.g., of master data are customer data, employee data, base rates for advances, FD rates, the rate for loans, penalty to be levied under different circumstances, etc.). Application software would access the database server. The data contained in the database must be very secure and no direct access should be permitted to prevent unauthorized changes. Strict discipline is followed regarding the maintenance of the database server, there is a designated role for maintenance of the database. The individual who performs this role is called the Database Administrator. His activities will also be monitored as all changes made would be recorded in a Log. Scrutiny of the log would disclose the type of activities and the effect of such activities.

Security aspects of database servers are an audit concern. Apart from the normal application server, the Automated Teller Machine Server (ATMS) and Internet Banking Application Server (IBAS) would also access the Database Server. It must
be noted that whatever be the operation that the customer has performed at the branch, through ATM, by Internet, mobile banking or any other alternate delivery channels, his account at the centralized database would be updated.

III. Automated Teller Machines (ATM) Channel Server

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

IV. Internet Banking Channel Server (IBCS)

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

V. Internet Banking Application Server

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

VI. 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.

VII. Proxy Server

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

VIII. 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.

B. 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. 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.

5.3 CORE BUSINESS PROCESSES FLOW AND 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 & 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.

5.3.1 Business process flow of Current & Savings Accounts (CASA)

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

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

<table>
<thead>
<tr>
<th>Current Account &amp; Savings Account - CASA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CASA Process - Understanding</strong></td>
</tr>
<tr>
<td>Customer</td>
</tr>
<tr>
<td>Customer applies for CASA facility through Internet banking/branch.</td>
</tr>
<tr>
<td>Customer ensures E-KYC documents are updated/uploaded.</td>
</tr>
<tr>
<td>Branch</td>
</tr>
<tr>
<td>RM basis the Customer request, proceeds the CASA Application after KYC Documents are shared.</td>
</tr>
<tr>
<td>KYC documents of the applicant are signed by the customer and shared to the bank.</td>
</tr>
<tr>
<td>RM basis the Customer request, sends the CASA application for along with the facilities requested for processing.</td>
</tr>
<tr>
<td>Risk Team</td>
</tr>
<tr>
<td>Risk Team assesses the customers background/credibility and allots the limits and facilities.</td>
</tr>
<tr>
<td>Decision Made by Credit/risk team.</td>
</tr>
<tr>
<td>Approved Application</td>
</tr>
<tr>
<td>Rejected Application</td>
</tr>
<tr>
<td>CASA Account Confirmation</td>
</tr>
<tr>
<td>On Confirmation of the Risk team, CASA account is opened in the customer account.</td>
</tr>
<tr>
<td>Customer</td>
</tr>
<tr>
<td>Customer makes use of facilities allotted with his CASA Account basis the Risk Approval.</td>
</tr>
<tr>
<td>Bank</td>
</tr>
</tbody>
</table>

Fig. 5.3.1: CASA Process

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

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

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

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

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

(b) **Risk & Controls around the CASA Process (discussed in the Table 5.3.1)**

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Risk</th>
<th>Key Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Credit Line setup is unauthorized and not in line with the banks policy.</td>
<td>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.</td>
</tr>
<tr>
<td>2.</td>
<td>Credit Line setup in CBS is unauthorized and not in line with the banks policy.</td>
<td>Access rights to authorize the credit limit in case of account setup system should be restricted to authorized personnel.</td>
</tr>
<tr>
<td>3.</td>
<td>Customer Master defined in CBS is not in accordance with the Pre-Disbursement Certificate.</td>
<td>Access rights to authorize the customer master in CBS should be restricted to authorized personnel.</td>
</tr>
<tr>
<td>4.</td>
<td>Inaccurate interest / charge being calculated in CBS.</td>
<td>Interest on fund based facilities are automatically calculated in the CBS as per the defined rules.</td>
</tr>
<tr>
<td>5.</td>
<td>Unauthorized personnel approving the CASA’s transaction in CBS.</td>
<td>Segregation of Duties to be maintained between the initiator and authorizer of the transaction for processing transaction in CBS.</td>
</tr>
<tr>
<td>6.</td>
<td>Inaccurate accounting entries generated in CBS.</td>
<td>Accounting entries are generated by CBS basis the facilities requested by the customer and basis defined configurations for those facilities in CBS.</td>
</tr>
</tbody>
</table>
5.3.2 Business Process flow of Credit Cards

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

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

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

(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, assess the financial and credit worthiness of the borrowers and issues a credit limit to the customer in CBS and allotted a credit card.

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

![Credit Card Process Diagram](image-url)
(b) Process Flow of Sale - Authorization process of Credit Card Facility (as shown in the Fig. 5.3.3)

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

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

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

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

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

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

© The Institute of Chartered Accountants of India
(c) **Process Flow of Clearing & Settlement process of Credit Card Facility (as shown in the Fig. 5.3.3)**

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

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

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

(d) **Risks and Controls around the Credit Card Process (Refer Table 5.3.2)**

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Risks</th>
<th>Key Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Credit Line setup is unauthorized and not in line with the banks policy.</td>
<td>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.</td>
</tr>
<tr>
<td>2.</td>
<td>Credit Line setup is unauthorized and not in line with the banks policy.</td>
<td>Access rights to authorize the credit limit in the credit card system should be restricted to authorized personnel.</td>
</tr>
<tr>
<td>3.</td>
<td>Masters defined for the customer are not in accordance with the Pre-Disbursement Certificate.</td>
<td>Access rights to authorize the customer master in credit card system should be restricted to authorized personnel, Segregation of duties exist in credit card system such that the system restricts the maker having checker rights to approve the facilities booked by self in the credit card system.</td>
</tr>
<tr>
<td>4.</td>
<td>Credit Line setup can be breached.</td>
<td>Transaction cannot be made if the aggregate limit of outstanding amount exceeds the credit limit assigned to customer.</td>
</tr>
<tr>
<td>5.</td>
<td>Inaccurate interest/charge being calculated in the Credit Card system.</td>
<td>Interest on fund based credit cards and charges are automatically calculated in the credit card system as per the defined masters.</td>
</tr>
<tr>
<td>6.</td>
<td>Inaccurate reconciliations performed.</td>
<td>Daily reconciliation for the balances received from credit card network with the transactions updated in the credit card system on card network level.</td>
</tr>
</tbody>
</table>

**5.3.3. 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.

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

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

(ii) Borrower / Customer approaches the bank for a mortgage and relationship manager/ loan officer explains the customer about home loan and its various feature. Customer to fill 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.
Fig. 5.3.4: Business process flow of Mortgages

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

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

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

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

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

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

(c) Risk & Controls around the Mortgage Process (discussed in the Table 5.3.3)

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Risk</th>
<th>Key Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Incorrect customer and loan details are captured which will affect the overall downstream process.</td>
<td>There is secondary review performed by an independent team member who will verify loan details captured in core banking application with offer letter.</td>
</tr>
<tr>
<td>2.</td>
<td>Incorrect loan amount disbursed.</td>
<td>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.</td>
</tr>
<tr>
<td>3.</td>
<td>Interest amount is incorrectly calculated and charged.</td>
<td>Interest amount is auto calculated by the core banking application basis loan amount, ROI and tenure.</td>
</tr>
<tr>
<td>4.</td>
<td>Unauthorized changes made to loan master data or customer data.</td>
<td>System enforced segregation of duties exist in the core banking application where the inputter of the transaction cannot approve its own transaction and reviewer cannot edit any details submitted by inputter.</td>
</tr>
</tbody>
</table>
5.3.4 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:

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

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

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

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

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

(b) **Process flow for Bank Treasury Operations:** Process flow for Bank Treasury Operations is provided in the Fig. 5.3.5.

![Fig. 5.3.5: Process flow for Bank Treasury Operations](image)
(c) **Risk & Controls around the Treasury Process:** (Listed in the Table 5.3.4)

**Table 5.3.4: Risk & Controls around the Treasury Process**

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Risk</th>
<th>Key Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Unauthorized securities setup in systems such as Front office/Back office.</td>
<td>Appropriate Segregation of duties and review controls around securities master setup/amendments.</td>
</tr>
<tr>
<td>2.</td>
<td>Inaccurate trade is processed.</td>
<td>Appropriate Segregation of duties and review controls to ensure the accuracy and authorization of trades.</td>
</tr>
<tr>
<td>3.</td>
<td>Unauthorized confirmations are processed.</td>
<td>Complete and accurate confirmations to be obtained from counter-party.</td>
</tr>
<tr>
<td>4.</td>
<td>Insufficient Securities available for Settlement</td>
<td>Effective controls on securities and margins.</td>
</tr>
<tr>
<td>5.</td>
<td>Incomplete and inaccurate data flow between systems.</td>
<td>Inter-system reconciliations, Interfaces and batch processing controls.</td>
</tr>
<tr>
<td>6.</td>
<td>Insufficient funds are available for settlements.</td>
<td>Controls at CCIL/NEFT/RTGS settlements to ensure the margin funds availability and the timely funds settlements.</td>
</tr>
<tr>
<td>7.</td>
<td>Incorrect Nostro payments processed.</td>
<td>Controls at Nostro reconciliation and payments.</td>
</tr>
</tbody>
</table>

**5.3.5 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 can be generally of following types:

- Cash Credits/Overdrafts
- Demand Loans/Term loans
- Bill Discounting
(ii) **Non-Fund Based Credit Facilities:** In this type of credit facility, the banks funds are not lent to the customer and they include Bank Guarantees and Letter of Credit.

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

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

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

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

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

(iv) Credit team verifies the document’s, assess 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 sends it to the disbursement team i.e. the team who is responsible for disbursing the loan amount to customer.

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

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

(II) **Loan Disbursal / Facility Utilization and Income Accounting**

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

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

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

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

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

Table 5.3.5: Risk & Controls around the Treasury Process

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Product</th>
<th>Income for banks</th>
<th>Accounting of Income</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Cash Credit / Overdraft</td>
<td>Interest on Cash Credits/ Overdraft balances.</td>
<td>Interest accrued on a daily basis at the agreed rates.</td>
</tr>
<tr>
<td>2.</td>
<td>Demand draft/ Term Loan’s</td>
<td>Interest on Demand draft/Term loan.</td>
<td>Interest accrued on a daily basis at the agreed rates.</td>
</tr>
<tr>
<td>3.</td>
<td>Bill Discounting</td>
<td>Discounting Income.</td>
<td>Interest accrued on a daily basis at the agreed rates.</td>
</tr>
</tbody>
</table>

© The Institute of Chartered Accountants of India
(b) Process flow for Fund based loans (Fig. 5.3.6)

1. Identifies Customers
   - Relationship Manager (RM)

2. Relevant documents
   - RM request from customers

3. Evaluates the documents and sanction limits
   - Credit Team

4. Customer accepts the sanction letter

5. No → Process ends

6. Yes → Prepares an PDC
   - Credit Team

7. Creates Masters in Loan Booking System
   - Disbursement team

8. Request received for New Loan
   - Manual Request Letter

9. Booking of Loans
   - Loan Booking System

10. Interest
    - Loan Booking System

11. Maturity
    - Loan Booking System

Fig. 5.3.6: Process Flow for Fund based Loans
(c) Process flow for Non-fund based loans (Fig. 5.3.7)

Identifies Customers
Relationship Manager (RM)

Relevant documents
RM request from customers

Evaluates the documents and sanction limits
Credit Team

Customer accepts the sanction letter

No

Process ends

Yes

Prepares an PDC
Credit Team

Creates Master in Loan Booking System
Disbursement team

Financial Statements

Sub Ledger
Loan Booking System

Customer Account

Contingent Asset

Contingent Liability

Commission Income

Request received for New facility
Manual Request Letter

Booking of facility
Loan Booking System

Commission
Loan Booking System

Maturity
Loan Booking System

DR
CR

DR
CR

DR
CR

Fig. 5.3.7: Process Flow for Non-Fund based Loans
© The Institute of Chartered Accountants of India
(d) Risk and Controls in the Loans and Advances Process: These are provided in the Table 5.3.6.

**Table 5.3.6: Risk & Controls in the Loans and Advances Process**

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Risk</th>
<th>Key Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Credit Line setup is unauthorized and not in line with the banks policy.</td>
<td>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.</td>
</tr>
<tr>
<td>2.</td>
<td>Credit Line setup is unauthorized and not in line with the banks policy.</td>
<td>Access rights to authorize the credit limit in Loan Booking system/CBS should be restricted to authorized personnel.</td>
</tr>
<tr>
<td>3.</td>
<td>Masters defined for the customer are not in accordance with the Pre Disbursement Certificate.</td>
<td>Access rights to authorize the customer master in Loan Booking system/CBS should be restricted to authorized personnel. Segregation of duties exist in Loan Disbursement system. The system restricts the maker having checker rights to approve the loan/facilities booked by self in loan disbursal system</td>
</tr>
<tr>
<td>4.</td>
<td>Credit Line setup can be breached in Loan disbursement system/CBS.</td>
<td>Loan disbursement system/CBS restricts booking of loans/facilities if the limits assigned to the customer is breached in Loan disbursement system/CBS.</td>
</tr>
<tr>
<td>5.</td>
<td>Lower rate of interest/Commission may be charged to customer.</td>
<td>Loan disbursement system/CBS restricts booking of loans/facilities if the rate charged to the customer are not as per defined masters in system.</td>
</tr>
<tr>
<td>6.</td>
<td>Facilities/Loan’s granted may be unauthorized/inappropriate.</td>
<td>Segregation of duties exist in Loan Disbursement system. The system restricts the maker having checker rights to approve the loan/facilities booked by self in loan disbursal system</td>
</tr>
<tr>
<td>7.</td>
<td>Inaccurate interest /charge being calculated in the Loan disbursal system.</td>
<td>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</td>
</tr>
</tbody>
</table>

**5.3.6 Internet Banking Process**

- The customer applies to the bank for such a facility. The user is provided with a User ID and Password. As is the best practice, the password is expected to be changed soon after the first log on.
- Internet facility could be used only by accessing the website of the bank. For accessing the website, naturally a browser like Internet Explorer, Firefox or Chrome is used.
- On access, user is directed to secure web server. The internet banking website is hosted on the web server. The web server is in the central data centre of the bank. Access to the web server is permitted only to authorised users.
To protect the web server from unauthorised 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 authorised port is permitted.

An individual who accesses the website of bank through the browser will be able to access the web server and there will be a display of the bank’s web page on the screen of the client’s computer.

The web page will also provide all information generally of interest to the public. The web page also will have a specified area wherein a mention of user ID and password will be made.

The password will not be displayed in plain text but will only be in an encrypted form.

The web server forwards the customer details to the internet banking applications server which in turn accesses the IDBS. The server has already the database of all the customers who have been provided with internet banking facility. For each customer, it would be having details about user ID and password.

The information received from the web server is verified with the data of the customer held in the internet banking (IBAS).

Should the information not tally, the message ‘access denied’ would appear giving the reason giving the ‘user ID/ password incorrect’. The customer realising the mistake may rectify the mistake and make another attempt.

Normally, three such attempts would be permitted. After three attempts, the customer will be logged out for security reasons. If more attempts are permitted, there is a possibility of a person just trying out different combination of user ID and password to break into the system.

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

(a) Password change
(b) Balance inquiry
(c) Fund transfer
(d) Request for cheque book
(e) Stop payment
(f) Copy of statement of account; and
(g) ATM/ Credit Card related queries

The customer then chooses one of the services from the list. The service requested is directed by the web server to the IBAS for processing. The IBAS will access the Internet Banking Database Server for further processing.
The Internet Banking Channel Server (IBCS) will retrieve the data from the central database server. The IBCS will be able to access the central database server only through a middleware and firewall. The middleware is expected to convert the data to suit the requirements of IBCS.

Internet banking database server then forwards the customer data to the IBAS which processes the transaction e.g., The statement of account from the central database server is made available to the Internet Banking Database Server (IBDS). The IBCS then sends the data to the IBAS. The IBAS then sends the same to the web browser (Internet Explorer).

The web server generates a dynamic web page for the service requested e.g., the accounts statement generated by the web server and presented to Internet Explorer (say) the information is then provided to the web browser in an encrypted form.

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

### 5.3.7 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. 5.3.8 highlights flow of transaction when a customer buys online from vendor’s e-commerce website. Here, the user logs in on the e-commerce web site, places an order and selects option of payment – Cards, or Internet Banking.

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

### 5.3.8 Risks associated with CBS

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

- **Ownership of Data/ process**: Data resides at the Data Centre. Establish clear ownership.
- **Authorization process**: Anybody with access to the CBS, including the customer himself, can enter data directly. What is the authorization process?
- **Authentication procedures**: 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 interface and application software.
- **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.
- **Access Controls**: Designing and monitoring access control is an extremely challenging task.
- **Incident handling procedures**: These may not be adequate considering the need for real-time risk management.
- **Change Management**: At application level and data level – Master files, transaction files and reporting software.

### 5.3.9 IT related Risks and mitigating Controls

Auditors are expected to be control experts. CBS software uses Technology platform to provide a complete range of banking services integrating bank and its branches and providing end-to-end services to customers. There are inherent risks of this technology deployment of CBS. Risk is what can go wrong and impede the enterprise from achieving its objective, and controls are countermeasures which help in mitigating the risks. Auditors need to understand the IT environment, business processes, related risks and controls and evaluate the controls are available, appropriate and adequate.
Hence auditors need to understand how CBS works, the inherent risks, implemented controls and evaluate the residual risks and consequent exposures. There are multiple ways in which risks can be assessed. From a business perspective, the risks that can be classified based on following Information criteria:

- **Efficiency**: Response is delayed resulting in dissatisfied stakeholder.
- **Effectiveness**: Process is ineffective and multiple runs consume time.
- **Reliability**: Users lose confidence in information system.
- **Confidentiality**: Due to loss of critical data.
- **Integrity**: Incomplete or inaccurate data due to errors in input or processing.
- **Availability**: Information system is not available when required.
- **Compliance**: The information system does not comply with legal, regulatory, contractual or internal compliance requirements.

In this section, sample listing of risks and controls relating to critical types of general controls and application controls are outlined.

I. **Data Centre and Network Operations**

The Data Centre and Network operations are comprised of the following sub-processes:

- **Backups and Restoring of data**: To be done on regular basis as per back up policy.
- **Job and Batch Scheduling and Processing**: Running of various types of transactions on regular basis as per pre-defined schedules. For example: Clearing of cheques, interest computation is done at specified intervals.
- **Monitoring of Applications and supporting Servers**: The Servers and applications running on them are monitored to ensure that servers, network connections and application software along with the interfaces are working continuously.
- **Value Add areas of Service Level Agreements (SLA)**: SLA with vendors are regularly reviewed to ensure that the services are delivered as per specified performance parameters.
- **User training and qualification of Operations personnel**: The personnel deployed have required competencies and skill-sets to operate and monitor the IT environment of CBS of bank.

Sample listing of Risks and Controls w.r.t Data Centre and Network Operations is available in Table 5.3.7.
Table 5.3.7: Sample Listing of Risks and Controls w.r.t Data Centre and Network Operations

<table>
<thead>
<tr>
<th>Risks</th>
<th>Key IT Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>The transaction may not be recorded completely or accurately, and the related items will be inaccurately or incompletely recorded.</td>
<td>Batch and online processing procedures are defined, executed and monitored for successful and timely completion. Any exception is reviewed and timely resolved.</td>
</tr>
<tr>
<td>Invalid items may be recorded or valid items may be inaccurately or incompletely recorded.</td>
<td>Access to automated job scheduling tools, and executable programs are defined to restrict to appropriate individuals as per job requirement.</td>
</tr>
<tr>
<td>Timely and adequate technical support may not be available and issues may not be resolved.</td>
<td>Entity has written agreement(s) with outside contractors and/or software vendors to provide for technical support, as needed. Management monitors compliance with these agreements.</td>
</tr>
<tr>
<td>User queries may not be timely and adequately resolved.</td>
<td>Help desk function exists to provide support on user queries regarding systems. Problems are recorded and the log for timely resolution of all such user queries is monitored.</td>
</tr>
<tr>
<td>Timely execution and complete processing and availability of data may not be ensured.</td>
<td>Performance and capacity utilization of the computer systems are measured, reported, and reviewed by management.</td>
</tr>
<tr>
<td>Unavailability of applications and data backups in the event of a disaster. It can also result in disclosure of sensitive information.</td>
<td>All tapes, manuals, guides are properly labelled and timely stored in a secured environmentally controlled location.</td>
</tr>
<tr>
<td>Data may be lost and systems may not be recoverable in the event of a serious system failure. This may result in regulatory/legal complaints, loss of reputation beside financial loss.</td>
<td>Schedule backup and storage of data is done periodically and appropriately. Management periodically reviews backups are done as per back up policy and meet business and legal requirements.</td>
</tr>
<tr>
<td>Backup may not be available if subject to some disaster, resulting in risk of data loss.</td>
<td>Backups are archived off-site.</td>
</tr>
</tbody>
</table>
II. Information Security

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

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

- **User Security Administration:** Refers to security for various users of information systems. The security administration policy documents define how users are created and granted access as per organization structure and access matrix. It also covers the complete administration of users right from creation to disabling of users is defined as part of security policy.

- **Application Security:** Refers to how security is implemented at various aspects of application right from configuration, setting of parameters and security for transactions through various application controls.

- **Database Security:** Refers to various aspects of implementing security for the database software.

- **Operating System Security:** Refers to security for operating system software which is installed in the servers and systems which are connected to the servers.

- **Network Security:** Refers to how security is provided at various layers of network and connectivity to the servers.

- **Physical Security:** Refers to security implemented through physical access controls.

Sample listing of Risks and Controls w.r.t Information Security is available in Table 5.3.8.

**Table 5.3.8: Sample Listing of Risks and Controls w.r.t Information Security**

<table>
<thead>
<tr>
<th>Risks</th>
<th>Key IT Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Significant information resources may be modified inappropriately,</td>
<td>Super user access or administrator passwords are changed on system installation and are available with administrator only.</td>
</tr>
<tr>
<td>disclosed without authorization, and/ or unavailable when needed.</td>
<td>Password of super user or administrator is adequately protected.</td>
</tr>
<tr>
<td>(e.g., they may be deleted without authorization).</td>
<td></td>
</tr>
<tr>
<td>Lack of management direction and commitment to protect information assets.</td>
<td>Security policies are established and management monitors compliance with policies.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Potential Loss of confidentiality, availability and integrity of data and system.</td>
<td>Vendor default passwords for applications systems, operating system, databases, and network and communication software are appropriately modified, eliminated, or disabled.</td>
</tr>
<tr>
<td>User accountability is not established.</td>
<td>All users are required to have a unique user id.</td>
</tr>
<tr>
<td>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.</td>
<td>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.)</td>
</tr>
<tr>
<td>Unauthorized viewing, modification or copying of data and/or unauthorized use, modification or denial of service in the system.</td>
<td>System owners authorize the nature and extent of user access privileges, and such privileges are periodically reviewed by system owners</td>
</tr>
<tr>
<td>Security breaches may go undetected.</td>
<td>Access to sensitive data is logged and the logs are regularly reviewed by management.</td>
</tr>
<tr>
<td>Potential loss of confidentiality, availability and integrity of data and system.</td>
<td>Physical access restrictions are implemented and administered to ensure that only authorized individuals can access or use information resources.</td>
</tr>
<tr>
<td>Inadequate preventive measure for key server and IT system in case of environmental threat like heat, humidity, fire, flood etc.</td>
<td>Environmental control like smoke detector, fire extinguisher, temperature maintenance devices and humidity control devices are installed and monitored in data center.</td>
</tr>
<tr>
<td>Unauthorized system or data access, loss and modification due to virus, worms and Trojans.</td>
<td>Network diagram is prepared and kept updated. Regular reviews of network security are performed to detect and mitigate network vulnerabilities.</td>
</tr>
</tbody>
</table>

### III. Application Software

As already discussed in the previous chapter, Application software is the life-blood of an enterprise as they process all core transactions of an enterprise. In case of banks, application software is akin to the circulatory system which ensures flow of information within the bank. All the core information systems of the bank which interfaces with customers are run using various modules of CBS
including other software developed in-house or procured from other vendors. It is important to understand risks pertaining to application software as they directly impact the bank’s operations.

Some of the key application risks are implementation of weak security; unauthorized access/changes to data; unauthorized Remote Access; inaccurate Information processing; erroneous of falsified data input; misuse by authorized end users; incomplete processing of data; untimely processing; communications systems failure; inadequate testing of systems and software; inadequate training and support and insufficient documentation.

(a) **Application Software - Risks and Controls:** Sample listing of Risks and Controls w.r.t Application Controls are in the Table 5.3.9.

**Table 5.3.9: Sample listing of Risks and Controls w.r.t Application Controls**

<table>
<thead>
<tr>
<th>Risks</th>
<th>IT Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interest may be incorrectly computed leading to incorrect recording of income/expenditure.</td>
<td>Interest is automatically correctly computed.</td>
</tr>
<tr>
<td></td>
<td>Digits are rounded off appropriately.</td>
</tr>
<tr>
<td></td>
<td>Interest is accurately accrued.</td>
</tr>
<tr>
<td>Inappropriate assignment of rate codes resulting in violation of business rules and/or loss of revenue.</td>
<td>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.</td>
</tr>
<tr>
<td>Absence of appropriate system validations may result in violation of business rules.</td>
<td>System validations have been implemented to restrict set up of duplicate customer master records.</td>
</tr>
<tr>
<td>Inappropriate reversal of charges resulting in loss of revenue.</td>
<td>System does not permit reversal of the charges in excess of the original amount charged.</td>
</tr>
<tr>
<td>Multiple liens in excess of the deposit value may result in inability to recover the outstanding in the event of a default.</td>
<td>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.</td>
</tr>
<tr>
<td>Inappropriate security or controls over system parameter settings resulting in unauthorized or incorrect changes to settings.</td>
<td>Access for changes made to the configuration, parameter settings is restricted to authorized user and require authorization/verification from another user.</td>
</tr>
<tr>
<td>Issue</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Failure to automate closure of NRE/ NRO accounts on change in residence status</td>
<td>On change of Customer status from NRI/ NRO to Resident on system, the system force the closure of accounts opened for that customer under NRE/NRO schemes, and to re-open the same under resident saving account schemes.</td>
</tr>
<tr>
<td>Inappropriate set up of accounts resulting in violation of business rules</td>
<td>The system parameters are set up as per business process rules of the bank.</td>
</tr>
<tr>
<td>Failure to levy appropriate charges resulting in loss of revenue</td>
<td>System does not permit closing of an account having zero balance without recovering the applicable account closure charges.</td>
</tr>
<tr>
<td>Inappropriate security or controls over file upload transactions resulting in intentional or inadvertent accounting errors</td>
<td>Automated file upload process to the NPA Provisioning System, exist eliminating the need for manual intervention.</td>
</tr>
<tr>
<td>Incorrect classification and provisioning of NPAs, resulting in financial misstatement</td>
<td>Configuration/ customization exists in the application to perform the NPA classification as per relevant RBI guidelines.</td>
</tr>
<tr>
<td>Failure to levy appropriate charges resulting in loss of revenue.</td>
<td>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</td>
</tr>
<tr>
<td>Duplicate asset records may be created. Ownership of asset may not be clearly established</td>
<td>Unique id is created for each asset. Each asset is assigned to specific business unit and user to establish ownership.</td>
</tr>
</tbody>
</table>

(b) **Application Software - Configuration, Masters, Transactions and Reports**

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

(i) **Configuration:** In the context of CBS software, **Configuration** refers to the way a software system is set up for use. Configuration is the first step after installing the software. This involves setting up various parameters (configuration) as per policies and business process rules. In newer technologies, such as plug-and-play, much of this configuration is performed automatically. However, in case of application software, this needs to be done. Most of the system software are also configured with default parameters which need to be modified. Configuration
will also enable how the products and services are distinguished from each other. For example, a common module of deposits can be modified as current with configuration, no interest is paid, any no. of transactions is allowed, service charges are levied, customer type as “not individual”, etc. The work flow for each of the products or services can also be configured. It is very critical to configure the software correctly as per specific policies, procedures and practices of the bank. The various modules of the banks such as advances, deposits, access rules, user creation, cash, treasury, etc. must be configured as deployed in the bank. Configuration could include both hardware and software parameters. Configuration will define how software will function and what menu options are displayed.

Some examples of configuration are given here:

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

(ii) Masters: In a CBS software, Masters refer to the setting parameters for various types of product and service type as per software modules used in the bank. The masters are also referred to as standing data as these are changed only when required and will require higher level of access. The parameter settings in the masters will drive how the software will process relevant transactions. For example, the interest parameters will be used for computing interest for various type of deposits/advances. After configuring the software, the masters are set up first time during installation and these are changed whenever the business process rules or values. For example: If RBI has changed the lending rates based on which bank has decided to change the interest rates for specific type of advances, the interest parameters are to be updated. Any changes to these data should be authorized by appropriate personnel and these are logged and captured in exception reports. For example, if NPA rules are changed by RBI, then bank should update the NPA parameters, then these changes will be logged and captured in a log file and will also be part of the exception report.

Some examples of masters are as follows:

- Customer Master for advances: Credit limit, loan period, interest rate, penal interest rate, security offered, sanction terms, customer details, etc.
- Deposit Master: Interest rate, type of deposit, service charges, period of interest computation, Minimum balance, withdrawal limits, a/c type (NRE/
- **Customer Master**: Customer type, details, address, PAN details,
- **Employee Master**: Employee Name, Id, designation, level, joining details, salary, leave, etc.
- **Income Tax Master**: Tax rates applicable, Slabs, frequency of TDS, etc.

(iii) **Transactions**: In the context of CBS software, **Transactions** refer to the actual transactions of various products and services which can be user using menus and functions and by customer through internet/mobile banking. The transactions are allowed based on user access and access authorization matrix set. For example, for each user, access to specific modules, type of transactions, and what they can do: entry, authorize or view would be possible. Some examples of transactions are given here:

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

(iv) **Reports**: Users at different levels used information which is processed by the computers. This information could be in form of reports which are periodically generated or on demand. These reports could be standard or adhoc reports. The 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. CBS Software also have development platform using which, the bank can develop specific reports as required on standard or on an ad hoc basis. Most of the compliance and MIS reports are developed/available by default in a CBS software. However, depending on the management style and information requirements reporting features would be used by 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
5.4 REPORTING SYSTEMS AND MIS, DATA ANALYTICS AND BUSINESS INTELLIGENCE

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

Risk Prediction for Basel III, based on Artificial Intelligence

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

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

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

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

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

5.5 APPLICABLE REGULATORY AND COMPLIANCE REQUIREMENTS

5.5.1 Banking Regulation Act

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

© The Institute of Chartered Accountants of India
Core Banking Systems

5.5.2 RBI Regulations

The Reserve Bank of India (RBI) was established on April 1, 1935 in accordance with the provisions of the Reserve Bank of India Act, 1934. The basic functions of the RBI include over shareholding and voting rights of shareholders; supervise the appointment of the boards and management; regulate the operations of banks; lay down instructions for audits; control moratorium, mergers and liquidation; issue directives in the interests of public good and on banking policy, and impose penalties. In 1965, the Act was amended to include cooperative banks under its purview by adding the Section 56. Cooperative banks, which operate only in one state, are formed and run by the state government. But, RBI controls the licensing and regulates the business operations. The Banking Act was a supplement to the previous acts related to banking.

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

I. **Negotiable Instruments Act-1881 (NI Act)**

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

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

The definition of a cheque in electronic form contemplates digital signature with or without biometric signature and asymmetric crypto system. Since the definition was inserted in the year 2002, 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.
Reserve Bank as: “to regulate the issue of Bank Notes and keeping of reserves with a view to securing monetary stability in India and generally to operate the currency and credit system of the country to its advantage.” The Primary objective of BFS is to undertake consolidated supervision of the financial sector comprising commercial banks, financial institutions and non-banking finance companies. Some of the key functions of RBI are given here.

- **Monetary Authority:** Formulates implements and monitors the monetary policy with the objective of maintaining price stability and ensuring adequate flow of credit to productive sectors.

- **Regulator and supervisor of the financial system:** Prescribes broad parameters of banking operations within which the country’s banking and financial system functions with the objective of maintaining public confidence in the system, protect depositors’ interest and provide cost-effective banking services to the public.

- **Issuer of currency:** Issues and exchanges or destroys currency and coins not fit for circulation with the objective to give the public adequate quantity of supplies of currency notes and coins and in good quality.

Banks provide 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.

### I. Impact of Technology in Banking

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

Earlier, technology was a tool and used in specific department of the bank but now with CBS, Technology has become 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.

![Technology and Business Process Components](image)

**Fig. 5.5.1: Technology and Business Process Components**

### 5.5.3 Money Laundering

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

Sec.3 of PML Act, 2002 defines ‘money laundering’ as: “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 and projecting it as untainted property shall be guilty of the offence of money-laundering”.

### I. Prevention of Money Laundering Act (PMLA)

Under Section 12 of PMLA, every banking company, financial institution and intermediary, (hereinafter referred to as such entities) is required to maintain a record of transactions as may be prescribed by rules and furnish information to the Director within such time as may be prescribed. The records to be maintained by such entities are set forth in rule 3 of PMLR. Such records include record of cash transactions of value more than 10 lakhs or its equivalent in foreign currency, integrally connected cash transactions taking place within a month, cash transactions where forged or counterfeit notes are involved and suspicious transactions of the nature described therein. Under rule 6 of PMLR, such records are to be maintained for a period of five years from the date of transaction.

© The Institute of Chartered Accountants of India
The key aspects of PMLA are as follows:

- Maintenance of record of all cash transactions above ₹ 10 lakhs.
- All series of cash transactions of value less than ₹ 10 lakhs integrally connected if they have taken place within a month (aggregate value above ₹ 10 lakhs).
- All cash transactions here forged or counterfeit notes have been used.
- All suspicious transactions made in cash or otherwise.

The period before which the transactions are to be reported to the Director are set forth in Rule 8 of PMLR. With respect to the transactions of 10 lakhs and more and the integrally connected transactions referred to above, the information should be submitted every month before the 15th day of the succeeding month. The information relating to forged or counterfeit notes is required to be submitted within seven days of the date of occurrence of the transaction. About suspicious transactions, principal officer of such entities is required to furnish the information in writing or fax or email to the Director within a period of seven working days on being satisfied that the transaction is suspicious.

The requirement of maintaining the records by such entities regarding the identity of their clients is prescribed in Rule 9 of PMLR. The documents that need to be obtained with respect to different kinds of clients such as individual, company, partnership, trust and other unincorporated association have been listed therein. Such entities are required to formulate and implement a client identification programme which incorporates the requirements of the said rule. They may have their own additional requirements as they may feel appropriate to determine the identity of the clients. A copy of the said identification programme is required to be forwarded to Director. The maintenance of records and reporting of transactions help in tracking transactions involving money laundering or the persons involved in such transactions. Under section 13 of PMLA, the Director is empowered (without prejudice to any other action that may be taken under PMLA) to impose a fine which shall not be less than 10 thousand but which may extend to 1 lakh for each failure. Since the imposition of fine by the Director is without prejudice to any other action that may be taken under PMLA it is possible that such entities may be exposed to penalty also under Section 63. In terms of Section 70 if the contravention is committed by such entities the officers in charge of and responsible to the conduct of the business of such entity at the relevant time are also liable to be proceeded with and punished. It is therefore clear that such entities should have a robust system of keeping track of the transactions of the nature referred to in Prevention of Money Laundering Act (PMLA) and Prevention of Money Laundering Rules (PMLR) and report the same within the prescribed period as aforesaid. Apart from the risk of penalty, this involves reputational risk for such entities.
II. Three stages of Money Laundering (Refer Fig. 5.5.2)

1. Placement

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

![Money Laundering Process Diagram]

Fig. 5.5.2: Money Laundering Process

2. Layering

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

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

III. 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.

IV. Financing of Terrorism

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

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

5.5.4 Information Technology Act

The Information Technology Act was passed in 2000 and amended in 2008. The ITA Rules were passed in 2011. The Act provides legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as “electronic commerce”, which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate
electronic filing of documents with the Government. The Act provides the legal framework for electronic governance by giving recognition to electronic records and digital signatures. It also deals with cyber-crime and facilitates electronic commerce. It also defined cyber-crimes and prescribed penalties for them. The Amendment Act 2008 provides stronger privacy data protection measures as well as implementing reasonable information security by implementing ISO27001 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.

I. Cyber Crimes

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

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

- Committing of a fraud by manipulation of the input, output, or throughput of a computer based system.
- Computer forgery, which involves changing images or data stored in computers,
- Deliberate damage caused to computer data or programs through virus programs or logic bombs,
- Unauthorized access to computers by ‘hacking’ into systems or stealing passwords, and,
- Unauthorized reproduction of computer programs or software piracy.

Cybercrimes have grown big with some countries promoting it to attack another country’s security and financial health.
Banking sector is prone to high risks by cyber criminals as banks deal with money and using technology, frauds can be committed across geographical boundaries without leaving a trace. Hence, CBS and banking software is expected to have high level of controls covering all aspects of cyber security.

II. Key Provisions of IT related offences

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

Section 43 provides for Penalty and compensation for damage to computer, computer system, etc.

If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network, or computer resource:

- Accesses or secures access to such computer, computer system or computer network;
- Downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
- Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
- Damages or causes to be damaged any computer, computer system or computer network, data, computer database or any other programs residing in such computer, computer system or computer network;
- Disrupts or causes disruption of any computer, computer system or computer network;
- Denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means; (g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;
- Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of
compensation to the person so affected.

- Destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;
- Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;

Section 65: Tampering with Computer Source Documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to 2 lakh rupees, or with both. The explanation clarifies “Computer Source Code” means the listing of programme, Computer Commands, Design and layout and program analysis of computer resource in any form.

Section 66: Computer Related Offences

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

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

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

Section 66-C: Punishment for identity theft

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

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

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

**Section 66-E: Punishment for violation of privacy**

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

**III. Sensitive Personal Data Information (SPDI)**

Section 43A of the IT Amendment Act imposes responsibility for protection of stakeholder information by body corporate. It states as follows: “Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource, which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, to the person so affected”.

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.

**IV. Privacy Policy**

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

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

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

5.6 SUMMARY

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

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

---

5.7 TEST YOUR KNOWLEDGE

5.7.1 Theoretical Questions

1. Briefly explain four steps of Risk Management Strategy?
   Refer Section 5.1.4.

2. Provide at least three examples each for Risks to Data and other IT risks in a Bank?
   Refer Section 5.1.4.

3. Provide four examples of indicators of higher IT risk in a bank.
   Refer Section 5.1.4.

4. Please explain and distinguish Internal Controls and IT controls in banks.
   Refer Section 5.1.4.

5. Explain key aspects of architecture of Core Banking Software (CBS).
   Refer Section 5.2.2.

6. Briefly explain core features of Core Banking Software.
Refer Section 5.2.3.

7. Briefly explain major components of a CBS solution.
   Refer Section 5.2.4.

8. Explain the CBS IT environment.
   Refer Section 5.2.4.

9. What are the risks associated with CBS software?
   Refer Section 5.3.8.

10. Please explain the four gateways for controlling Core banking software.
    Refer Section 5.3.9.

11. Please explain briefly the impact of Technology in Banking?
    Refer Section 5.5.2.

12. What are the key provisions of Prevention of Money Laundering Act (PMLA)?
    Refer Section 5.5.3.

13. Briefly explain all the stages of Money Laundering and how banks are used in laundering money.
    Refer Section 5.5.3.

14. What are Computer-related offences as per IT Act which impact banking?
    Refer Section 5.5.4.

**5.7.2 Multiple Choice Questions**

1. Which of the following is not a core banking services?
   (a) Advances  
   (b) Letters of Credit  
   (c) Reporting  
   (d) Deposits

2. Which of the following is an application control?
   (a) Configuring system software  
   (b) Setting parameters in masters  
   (c) Transaction Logging  
   (d) Back up of data

3. Which of the following is a General control?
   (a) Setting Database Security  
   (b) Edit checks
4. Which of the following is a core feature of CBS?
   (a) On-line real-time processing
   (b) Transactions are posted in batches
   (c) Databases are maintained as per branch
   (d) Loan processing is done at branch

5. Which of the following is one of the primary objective of implementing controls?
   (a) All computer errors are prevented
   (b) Frauds are detecting pro-actively
   (c) Undesired events are prevented or detected and corrected
   (d) Revenue targets are achieved

6. Which of the following best defines a risk?
   (a) Undesired events are prevented
   (b) Inherent vulnerabilities are identified
   (c) Physical threats are documented
   (d) Threat exploits vulnerability

7. Which of the following best defines Money Laundering?
   (a) Converting proceeds of crime and projecting it as untainted property
   (b) Tax Planning as per provision of IT Act
   (c) Gifting immoveable property to relatives
   (d) Transferring fixed deposit to employees

8. Which of the following is not computer related offence as per in IT Act, 2000?
   (a) Identify theft
   (b) Stealing of mobile
   (c) Stealing computer resource
   (d) Violation of privacy

9. What is the primary objective of SPDI?
   (a) Protecting computer software
   (b) Securing critical information
   (c) Securing Personal Information
10. Which of the following is a cybercrime?

(a) Breaking into ATM
(b) Physical theft at branch
(c) Software piracy
(d) Altering name in demand draft

Answers

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(c)</td>
<td>2</td>
<td>(c)</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>(a)</td>
<td>4</td>
<td>(a)</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>(c)</td>
<td>6</td>
<td>(d)</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>(a)</td>
<td>8</td>
<td>(b)</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>(c)</td>
<td>10</td>
<td>(c)</td>
<td></td>
</tr>
</tbody>
</table>