INTERMEDIATE COURSE

STUDY MATERIAL

PAPER : 7A

Enterprise Information Systems

BOARD OF STUDIES

THE INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA

This study material has been prepared by the faculty of the Board of Studies. The objective of the study material is to provide teaching material to the students to enable them to obtain knowledge in the subject. In case students need any clarifications or have any suggestions to make for further improvement of the material contained herein, they may write to the Director of Studies.

All care has been taken to provide interpretations and discussions in a manner useful for the students. However, the study material has not been specifically discussed by the Council of the Institute or any of its Committees and the views expressed herein may not be taken to necessarily represent the views of the Council or any of its Committees.

Permission of the Institute is essential for reproduction of any portion of this material.

Edition	:	July, 2019
Website	:	www.icai.org
E-mail	:	bosnoida@icai.org
Committee/Department	:	Board of Studies
ISBN No.	:	
Price (All Modules):		₹
Published by	:	The Publication Department on behalf of The Institute of Chartered Accountants of India, ICAI Bhawan, Post Box No. 7100, Indraprastha Marg, New Delhi 110 002, India.
Printed by	:	

BEFORE WE BEGIN….

The traditional role of a chartered accountant restricted to accounting and auditing, has now changed substantially and there has been a marked shift towards strategic decision making and entrepreneurial roles that add value beyond traditional financial reporting. The primary factors responsible for the change are the increasing business complexities on account of plethora of laws, borderless economies consequent to giant leap in e-commerce, emergence of new financial instruments, emphasis on corporate social responsibility, significant developments in information technology, to name a few. These factors necessitate an increase in the competence of chartered accountants to take up the role of not merely an accountant, auditor or more specifically an IS Auditor, but a global solution provider. Towards this end, the scheme of education and training is being continuously reviewed so that it is in sync with the requisites of the dynamic global business environment; the competence requirements are being continuously reviewed to enable aspiring chartered accountants to acquire the requisite professional competence to take on new roles.

Under the Revised Scheme of Education and Training, at the Intermediate Level, you are expected to not only acquire professional knowledge but also the ability to apply such knowledge in problem solving. Recognizing the importance of Information Technology in today's era, Chartered Accountancy course has included the subject as a part of the course curriculum at Intermediate Level. The process of learning should help you inculcate the requisite IT skill-sets necessary for achieving the desired professional competence. A paper on 'Enterprise Information Systems' forming the part of curriculum at Intermediate level of the Chartered Accountancy course is to provide the understanding of the fundamental concepts of Information systems and business process flows, Financial and Accounting systems, Core Banking Systems and e-commerce and m-commerce transactions.

The overall learning objective of this paper ***"To develop an understanding of technology enabled Information Systems and their impact on enterprise-wide processes, risks and controls"*** has been kept in mind while developing the material. The content for each chapter in the study material has been structured in the following manner:

(i) **Learning Outcomes :** Learning outcomes which you need to demonstrate after learning each topic have been detailed in the first page of each chapter/unit. Demonstration of these learning outcomes would help you to achieve the desired level of technical competence.

(ii) **Chapter Overview:** As the name suggests, this chart/table would give a broad outline of the contents covered in the chapter.

(iii) **Introduction:** A brief introduction is given at the beginning of each chapter which would help you get a feel of the topic.

(iv) **Content:** The concepts are explained in student-friendly manner and illustrated with the aid of examples/illustrations/diagrams/tables. These value additions would help you develop conceptual clarity and get a good grasp of the topic.

(v) **Let us recapitulate:** A summary of the chapter is given at the end to help you revise what you have learnt. It would especially help you to revise the chapter quickly the day before the examination.

(vi) **Test your Knowledge:** This comprises of Theory Questions and Multiple Choice Questions which test the breadth and depth of your understanding of the entire syllabus.

Chapter-wise coverage of various topics in the study material are as follows:

♦ **Chapter 1 - Automated Business Processes** introduces the concept of Business Processes and the impact of their automation with the help of Technology. The chapter focuses on Enterprise Risk Management, associated risks and their corresponding mitigating controls for some specific business processes like P2P, O2C etc. Further, it provides an insight to the mapping systems like Flowcharts and Data Flow Diagrams (DFDs).

♦ **Chapter 2 - Financial and Accounting Systems** familiarizes with the concept of integrated and Non-integrated systems and the Financial and Accounting systems as an Integrated system. It further discusses at length various business process modules and data flow involved in the system and their related risks and controls. The significance of XBRL and Reporting systems are also emphasized with the applicable regulatory and compliance requirements for the automated systems.

♦ **Chapter 3 - Information Systems and Its Components** disseminates the basic concept of Information Systems and its components – People, Computer System, Data Resources, and Networking and Communication System. The chapter deals with controls, their need and classification of Information Systems' Controls on different perspectives. The objectives while Auditing Information Systems and their controls with an in-depth discussion on Organization structure and Responsibilities are well emphasized upon.

- **Chapter 4 - E-Commerce, M-Commerce and Emerging Technologies** provides the meaning, components, architecture and process flows involved in E-commerce with a basic understanding on the paradigms of various Computing Technologies like Cloud Computing, Grid Computing, Mobile Computing, Green Computing and BYOD etc.

- **Chapter 5 - Core Banking Systems** brings into light the core concepts of CBS that includes the components and architecture of CBS and impact of related risks and controls. Furthermore, the chapter highlights various regulatory and compliance requirements applicable to CBS such as Banking Regulations Act, RBI regulations, Prevention of Money Laundering Act and Information Technology Act.

This study material covers both concepts and practical aspects and hence, you are advised to read the study material not only from examination point of view but also from practical perspective of how this is relevant and can be applied in any work environment.

HAPPY READING AND BEST WISHES!

SYLLABUS

PAPER – 7A : ENTERPRISE INFORMATION SYSTEMS

(50 MARKS)

OBJECTIVE

"To develop an understanding of technology enabled Information Systems and their impact on enterprise-wide processes, risks and controls."

CONTENTS

1. AUTOMATED BUSINESS PROCESSES

(i) Introduction to Enterprise Business Processes, Benefits, Risks and Controls.

(ii) Diagrammatic representation of business processes using Flowcharts.

(iii) Risks and controls for specific business processes: Procure to pay (P2P), Order to Cash, Inventory Cycle, Hire to Retire, Supply Chain Management, Fixed As- sets etc.

(iv) Applicable regulatory and compliance requirements including computer related offences, privacy, cyber-crime, Sensitive Personal Data Information of Information Technology Act, 2000.

2. FINANCIAL AND ACCOUNTING SYSTEMS

(i) Integrated (ERP) and non-integrated systems with related risks and controls.

(ii) Business process modules and their integration with Financial and Accounting systems.

(iii) Reporting Systems and MIS, Data Analytics and Business Intelligence.

(iv) Business Reporting and fundamentals of XBRL (eXtensible Business Reporting Language).

(v) Applicable regulatory and compliance requirements.

3. INFORMATION SYSTEMS AND ITS COMPONENTS

(i) Components of Automated Information Systems: Application Systems, Data- base, Network and Operating System with related risks and controls.

(ii) Mapping of Organization structure with segregation of duties in Information Systems.

4. E-COMMERCE, M-COMMERCE AND EMERGING TECHNOLOGIES

(i) Components and Architecture of E-Commerce and M-Commerce with related risks and controls.

(ii) Business process flow with its related risks and controls.

(iii) Applicable regulatory and compliance requirements.

(iv) Emerging technologies with its related risks and controls.

5. CORE BANKING SYSTEMS

(i) Components and Architecture of CBS and related risks and controls.

(ii) Core modules of banking and Business process flow and its related risks and controls.

(iii) Reporting Systems and MIS, Data Analytics and Business Intelligence.

(iv) Applicable regulatory and compliance requirements.

SIGNIFICANT ADDITIONS IN 2019 EDITION OVER 2017 EDITION

Chapter	Sections/Sub Sections wherein major Additions have been done	Page Numbers
Chapter 1: Automated Business Processes	Fig. 1.1.1: Customer Service Department Activities	1.4
	Table 1.2.1: Example representing all categories of Business Processes	1.6 – 1.7
	1.4.2 Sources of Risk	1.19
	1.4.3 Types of Risks	1.19 – 1.20
	1.4.4 Risk Management and Related Terms	1.22 – 1.25
	1.4.5 Risk Management Strategies	1.25 – 1.26
	1.5.4 Framework of Internal Control as per Standards on Auditing	1.31 - 1.33
	1.6.2 Enterprise Risk Management Framework	1.36
	1.7.1 Introduction to Flowcharts – Ex(s) 3, 4, 5	1.44 – 1.49
Chapter 2: Financial and Accounting Systems	Table 2.2.5: Installed and Cloud Based Application	2.17 – 2.19
	2.2.6 Benefits of an ERP System	2.21 – 2.23
	2.3.2 ERP Implementation, its Risks and related Controls	
	• Table 2.3.1(A): Risks and corresponding Controls related to People Issues	2.26 – 2.27
	• Table 2.3.1(B): Risks and corresponding Controls related to Process Risks	2.28
	• Table 2.3.1(C): Risks and corresponding Controls related to Technological Risks	2.28 – 2.29
	• Table 2.3.1(D): Risks and corresponding Controls related to some other	2.29 -2.30

	implementation issues • Table 2.3.1(E): Risks and corresponding Controls related to post- implementation issues	2.30
	2.6.3 ERP - Business Process Modules (BPM)	
	b. Controlling Module	2.42 – 2.43
	e. Production Planning (PP) Module	2.46 – 2.47
	g. Quality Management Module	2.49 – 2.50
	h. Plant Maintenance Module	2.51
	i. Project Systems Module	2.52 – 2.53
	j. Supply Chain Module	2.53 – 2.54
	2.8.3 Business Intelligence (BI)	2.65 – 2.66
Chapter 3: Information Systems and its components	3.3.3 Data Resources • Big Data	3.17
Chapter 4: E-Commerce, M-Commerce and Emerging Technologies	4.1.5 E-Commerce Business Models	4.10 – 4.13
	4.8.7 Web 3.0	4.75
	4.8.8 Internet of Things (IoT)	4.77 – 4.78
Chapter 5: Core Banking Systems	5.1.3 Overview of Core Banking Systems	5.12 – 5.14
	5.3.1 Risks associated with CBS	5.25 – 5.27
	5.5.4 Banking Regulation Acts	
	• Prevention of Money Laundering Act	5.60 – 5.64
	• Information Technology Act A. Key Provisions of IT Act	5.65 – 5.69

CONTENTS

SECTION A: ENTERPRISE INFORMATION SYSTEMS

CHAPTER 1: AUTOMATED BUSINESS PROCESSES

CHAPTER 2: FINANCIAL AND ACCOUNTING SYSTEMS

CHAPTER 3: INFORMATION SYSTEMS AND ITS COMPONENTS

CHAPTER 4: E-COMMERCE, M-COMMERCE AND EMERGING TECHNOLOGIES

CHAPTER 5: CORE BANKING SYSTEMS

CHAPTER 1

AUTOMATED BUSINESS PROCESSES

LEARNING OUTCOMES

After reading this chapter, you will be able to -

❑ Build an understanding on the concepts of Business Process, its automation and implementation.

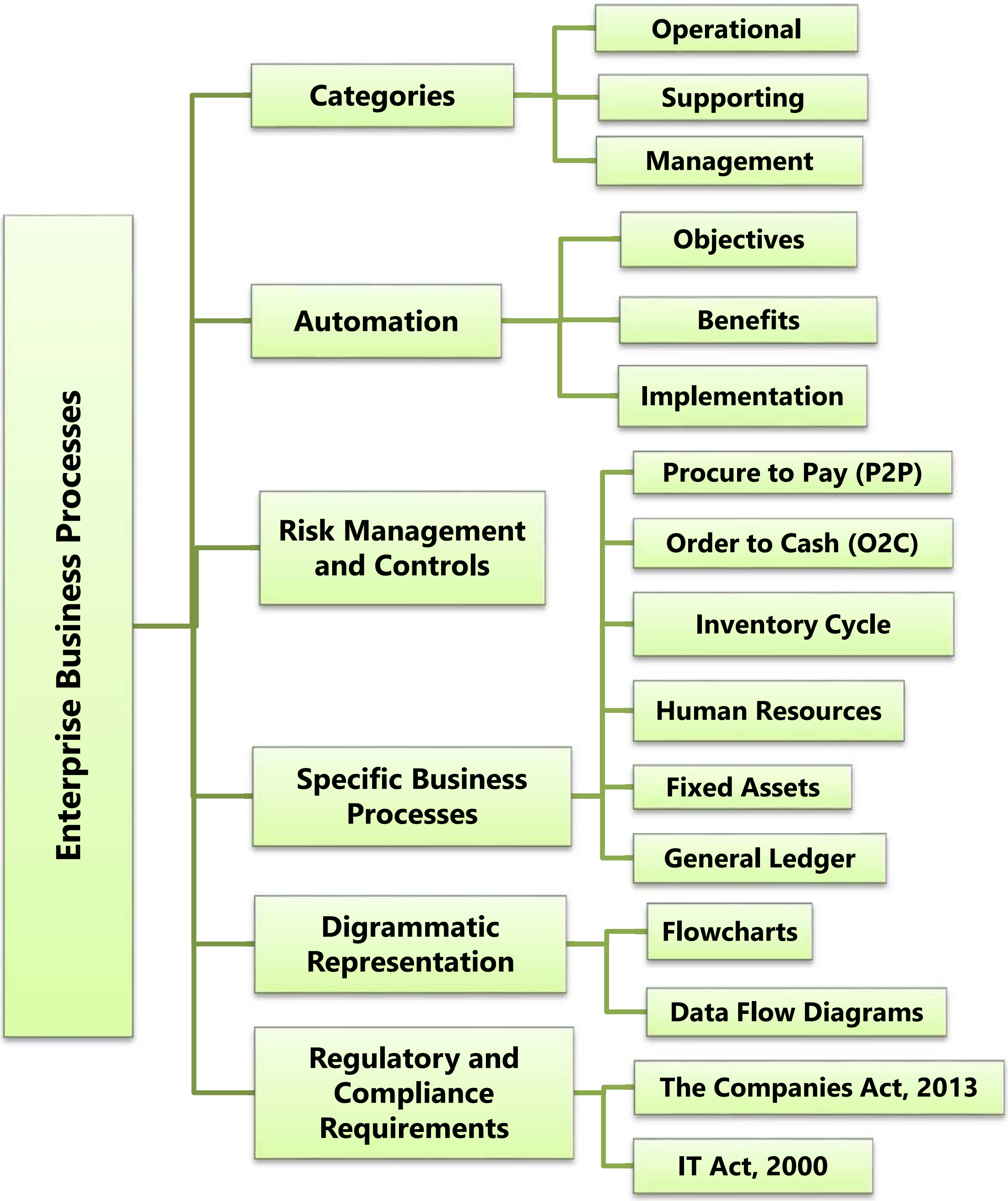
❑ Understand concepts, flow and relationship of internal and automated controls.

❑ Acknowledge risks and controls of various business processes.

❑ Grasp the understanding on the structure and flow of business processes, related risks and controls.

❑ Comprehend the specific regulatory and compliance requirements of The Companies Act and The Information Technology Act as applicable to Enterprise Information Systems.

CHAPTER OVERVIEW



1.1 INTRODUCTION

In today's connected world where information flows at speed of light, success on any organization depends on its ability to respond to fast changing environment. The capability of any organization depends on its ability to take fast decisions. A large organization typically has several different kinds of Information systems built around diverse functions, organizational levels, and business processes that can automatically exchange information. All these information systems have fragmentation of data in hundreds of separate systems, degrades organizational efficiency and business performance. For instance – sales personnel might not be able to tell at the time they place an order whether the ordered items are in inventory, and manufacturing cannot easily use sales data to plan for next production.

The solution to this problem is provided by Enterprise Information Systems, by collecting data from numerous crucial business processes like manufacturing and production, finance and accounting, sales and marketing, and human resources and storing the data in single central data repository. An **Enterprise Information System (EIS)** may be defined as any kind of information system which improves the functions of an enterprise business processes by integration.

An EIS provide a technology platform that enables organizations to integrate and coordinate their business processes on a robust foundation. An EIS provides a single system that is central to the organization that ensures information can be shared across all functional levels and management hierarchies. It may be used to amalgamate existing applications. An EIS can be used to increase business productivity and reduce service cycles, product development cycles and marketing life cycles. Other outcomes include higher operational efficiency and cost savings.

For example, when a customer places an order, the data flow automatically to other fractions of the company that are affected by them leading to the enhanced coordination between these different parts of the business which in turn lowers costs and increase customer satisfaction. Refer to the Fig. 1.1.1.

- The order transaction triggers the warehouse to pick the ordered products and schedule shipment.
- The warehouse informs the factory to replenish whatever has depleted.
- The accounting department is notified to send the customer an invoice.
- Debtors Department keeps track of payments.

- Customer service representatives track the progress if the order through every step to inform customers about the status of their orders.

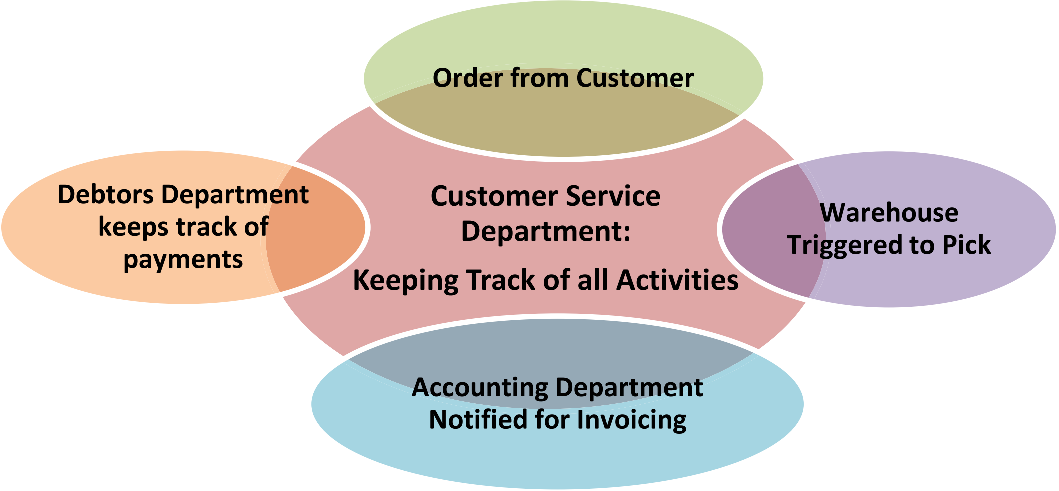

Order from Customer
Debtors Department keeps track of payments
Customer Service Department:
Keeping Track of all Activities
Warehouse Triggered to Pick
Accounting Department Notified for Invoicing

Fig. 1.1.1: Customer Service Department Activities

1.2 ENTERPRISE BUSINESS PROCESSES

A **Business Process** is an activity or set of activities that will accomplish a specific organizational goal. Business processes are designed as per vision and mission of top management. Business processes are reflection of entities management thought process. The success or failure of an organization is dependent on how meticulously business processes have been designed and implemented.

Business Process Management (BPM), helps an organization achieve 3E's for business processes, namely **Effectiveness**, **Efficiency** and **Economy**. BPM is a systematic approach to improving these processes. Business Process Management is an all-round activity working on a 24x7 basis to ensure improvement in all parameters all the time. The key components of business process are outlined below in the Fig.1.2.1.

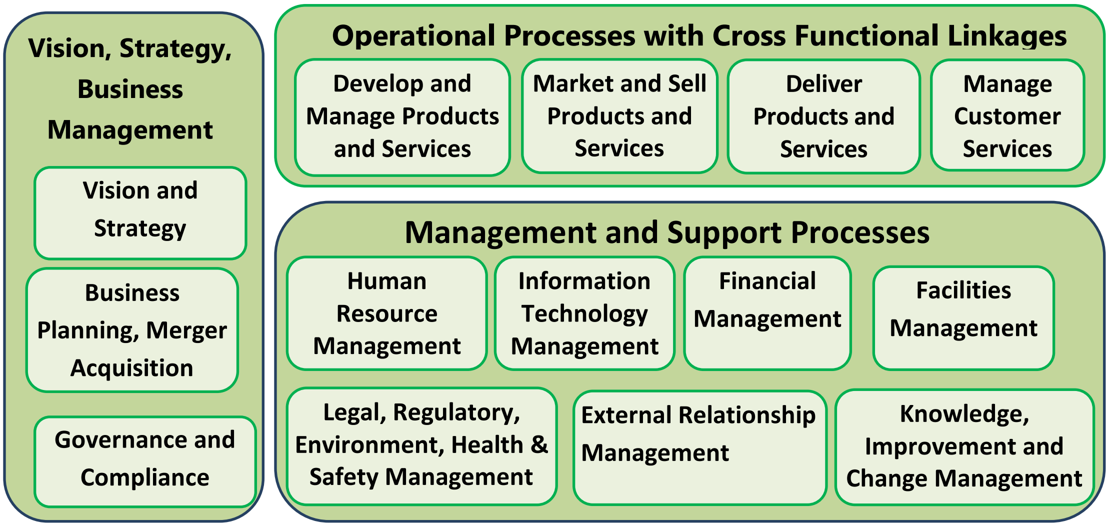

Vision, Strategy, Business Management
Vision and Strategy
Business Planning, Merger Acquisition
Governance and Compliance
Operational Processes with Cross Functional Linkages
Develop and Manage Products and Services
Market and Sell Products and Services
Deliver Products and Services
Manage Customer Services
Management and Support Processes
Human Resource Management
Information Technology Management
Financial Management
Facilities Management
Legal, Regulatory, Environment, Health & Safety Management
External Relationship Management
Knowledge, Improvement and Change Management

Fig. 1.2.1: Enterprise Business Process Model

The key guiding factor for any business process shall be top management vision and mission. This vision and mission shall be achieved through implementing <u>Operational</u>, <u>Support</u> and <u>Management</u> services. These are referred to as categories of business process.

1.2.1 Categories of Business Processes

Depending on the organization, industry and nature of work; business processes are often broken up into different categories as shown in the Fig. 1.2.2.

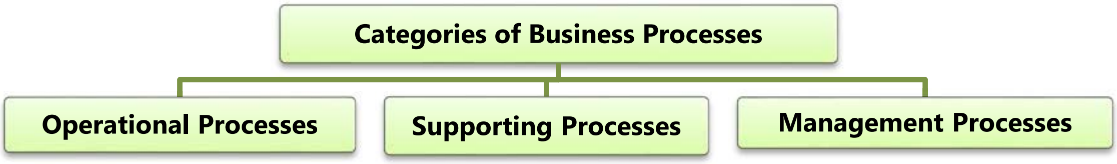


Fig. 1.2.2: Categories of Business Processes

I. Operational Processes (or Primary Processes)

Operational or **Primary Processes** deal with the core business and value chain. These processes deliver value to the customer by helping to produce a product or service. Operational processes represent essential business activities that accomplish business objectives, eg. generating revenue - Order to Cash cycle (O2C), Procurement – Purchase to Pay (P2P) cycle.

II. Supporting Processes (or Secondary Processes)

Supporting Processes back core processes and functions within an organization. Examples of supporting or management processes include Accounting, Human Resource (HR) Management and workplace safety. One key differentiator between operational and support processes is that support processes do not provide value to customers directly. However, it should be noted that hiring the right people for the right job has a direct impact on the efficiency of the enterprise.

Human Resource Management (Example)

The main HR Process Areas are grouped into logical functional areas - Recruitment and Staffing; Goal Setting; Training and Development; Compensation and Benefits; Performance Management; Career Development and Leadership Development.

III. Management Processes

Management Processes measure, monitor and control activities related to business procedures and systems. Examples of management processes include internal communications, governance, strategic planning, budgeting, and infrastructure or capacity management. Like supporting processes, management processes do not provide value directly to the customers. However, it has a direct impact on the efficiency of the enterprise.

Budgeting (Example)

Referring to the Fig. 1.2.3, in any enterprise, budgeting needs to be driven by the vision (what enterprise plans to accomplish) and the strategic plan (the steps to get there). Having a formal and structured budgeting process is the foundation for good business management, growth and development.

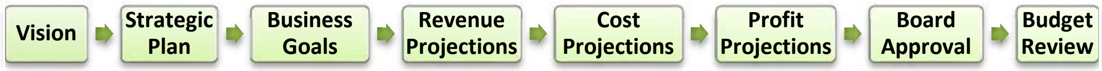


Fig. 1.2.3: Budgeting Process

Table 1.2.1 summarises various categories of Business Processes through an example.

Table 1.2.1: Example representing all categories of Business Processes

S. No.	***Nature of Business Decision***	***Description of decision***
1	***Vision and Mission***	***One of Asia's largest dairy product companies decided in 2005 to increase its turnover by 2X in next ten years. The present turnover was ₹10,000/- Crores.***

2	***Management Process***	***The top management sat down and listed activates to be done to achieve the said turnover. This included:*** - ***Enter into new markets. It was decided to have an all India presence. At present the company products were being sold across 20 out of 25 states and all state capital excluding the four metros, namely Delhi, Mumbai, Chennai and Kolkata.*** - ***Launch new products. Presently the company was mainly selling milk products. Few new products that were decided to be sold in future included; Biscuits, Toast, Atta, Packaged Drinking Water.*** - ***Acquire existing dairies in markets where company had no presence.***
3	***Support Process***	***For all activities to be done as envisioned by top management, a huge effort was needed on human resources front. This included -*** - ***Defining and creating a new management structure*** - ***Performing all human resource activities as listed above.***
4	***Operational Process***	***Post the management processes, it is on the operational managers to implement the decisions in actual working form. It is here where the whole hard job is done.***

1.3 AUTOMATED BUSINESS PROCESSES

Today technology innovations are increasing day by day, technology is becoming easily available, cost of accessing and using technology is going down, internet connectivity in term of speed and geographical spread is increasing day by day. All these factors are having a profound impact on the business processes being used by entity.

In the days of manual accounting, most business processes were carried out manually. For example, a sales invoice would be raised manually and based on the shipment of goods the inventory would be manually updated for reducing the stock. Subsequently the accounting entries would be manually passed by debiting and crediting the respective accounts, through journal entries. Today most of the business processes have been automated to make enterprises more efficient and to handle the large volumes of transactions in today's world. This is what has led to **Business Process Automation (BPA).** The manual example given above would be performed in an integrated computer system as follows:

- Raise invoice to customer in a computer system using relevant application software;
- The system automatically reduces the stock;
- The system instantly passes the necessary accounting entries by adding relevant transactions in relevant database tables:
  - Debit: Customer
  - Credit: Sales, Indirect Taxes
  - Debit: Cost of Goods Sold
  - Credit: Inventory

Business Process Automation (BPA) is the technology-enabled automation of activities or services that accomplish a specific function and can be implemented for many different functions of company activities, including sales, management, operations, supply chain, human resources, information technology, etc. In other words, BPA is the tactic a business uses to automate processes to operate efficiently and effectively. It consists of integrating applications and using software applications throughout the organization. BPA is the tradition of analyzing, documenting, optimizing and then automating business processes.

1.3.1 Factors affecting BPA success

The success of any Business Process Automation shall only be achieved when BPA ensures the following:

- **Confidentiality:** To ensure that data is only available to persons who have right to see the same;
- **Integrity:** To ensure that no un-authorized amendments can be made in the data;
- **Availability:** To ensure that data is available when asked for; and
- **Timeliness:** To ensure that data is made available in at the right time.

To ensure that all the above parameters are met, BPA needs to have appropriate internal controls put in place.

1.3.2 Benefits of Automating Business Process

The business process is the flow of information, customized by value-added tasks, that begins with the primary contact with a potential customer and continues through deliverance of a finished product. Well-developed business processes can generate a flawless link from initial customer interface through the supply chain.

Automation of those processes maintains the accuracy of the information transferred and certifies the repeatability of the value-added tasks performed. Table 1.3.1 elaborates on major benefits of automating Business Processes.

Table 1.3.1: Benefits of Automating Business Processes

Quality and Consistency
♦ Ensures that every action is performed identically - resulting in high quality, reliable results and stakeholders will consistently experience the same level of service.
Time Saving
♦ Automation reduces the number of tasks employees would otherwise need to do manually. ♦ It frees up time to work on items that add genuine value to the business, allowing innovation and increasing employees' levels of motivation.
Visibility
♦ Automated processes are controlled and they consistently operate accurately within the defined timeline. It gives visibility of the process status to the organization.
Improved Operational Efficiency
♦ Automation reduces the time it takes to achieve a task, the effort required to undertake it and the cost of completing it successfully. ♦ Automation not only ensures systems run smoothly and efficiently, but that errors are eliminated and that best practices are constantly leveraged.
Governance & Reliability
♦ The consistency of automated processes means stakeholders can rely on business processes to operate and offer reliable processes to customers, maintaining a competitive advantage.
Reduced Turnaround Times
♦ Eliminate unnecessary tasks and realign process steps to optimize the flow of information throughout production, service, billing and collection. This adjustment of processes distils operational performance and reduces the turnaround times for both staff and external customers.

Reduced Costs
♦ Manual tasks, given that they are performed one-at-a-time and at a slower rate than an automated task, will cost more. Automation allows us to accomplish more by utilizing fewer resources.

1.3.3 BPA Implementation

Business needs a reason to go for any new system. Benefits outlined in Table 1.3.1 are good indicators why any business shall go for automation for business process. Of all good reasons discussed above, one factor needs additional consideration that is global competition. Today the connected world has opened huge opportunities as well as brought new threats to any business. The increased availability of choice to customers about products / services makes it very important for businesses to keep themselves updated to new technology and delivery mechanisms. All these factors are forcing businesses to adopt BPA.

The steps to go about implementing Business Process Automation are depicted in Table 1.3.2. One important point to remember is that not all processes can be automated at a time. The best way to go about automation is to first understand the criticality of the business process to the enterprise. Let us discuss the key steps in detail.

(i) Step 1: Define why we plan to implement a BPA?

The primary purpose for which an enterprise implements automation may vary from enterprise to enterprise. A list of generic reasons for going for BPA may include any or combination of the following:

- Errors in manual processes leading to higher costs.
- Payment processes not streamlined, due to duplicate or late payments, missing early pay discounts, and losing revenue.
- Paying for goods and services not received.
- Poor debtor management leading to high invoice aging and poor cash flow.
- Not being able to find documents quickly during an audit or lawsuit or not being able to find all documents.
- Lengthy or incomplete new employee or new account on-boarding.
- Unable to recruit and train new employees, but where employees are urgently required.

- Lack of management understanding of business processes.
- Poor customer service.

(ii) Step 2: Understand the rules / regulation under which enterprise needs to comply with?

One of the most important steps in automating any business process is to understand the rules of engagement, which include following the rules, adhering to regulations and following document retention requirements. This governance is established by a combination of internal corporate policies, external industry regulations and local, state, and central laws. Regardless of the source, it is important to be aware of their existence and how they affect the documents that drive the processes. It is important to understand that laws may require documents to be retained for specified number of years and in a specified format. Entity needs to ensure that any BPA adheres to the requirements of law.

(iii) Step 3: Document the process, we wish to automate

At this step, all the documents that are currently being used need to be documented. The following aspects need to be kept in mind while documenting the present process:

- What documents need to be captured?
- Where do they come from?
- What format are they in: Paper, FAX, email, PDF etc.?
- Who is involved in processing of the documents?
- What is the impact of regulations on processing of these documents?
- Can there be a better way to do the same job?
- How are exceptions in the process handled?

The benefit of the above process for user and entity being:

- It provides clarity on the process.
- It helps to determine the sources of inefficiency, bottlenecks, and problems.
- It allows designing the process to focus on the desired result with workflow automation.

An easy way to do this is to sketch the processes on a piece of paper, possibly in a flowchart format. Visio or even Word can be used to create flowcharts easily.

It is important to understand that no automation shall benefit the entity, if the process being automated is error-prone. Investment in hardware, workflow software and professional services, would get wasted if the processes being automated are not made error-free. Use of technology needs to be made to realize the goal of accurate, complete and timely processing of data so as to provide right information to the right people safely and securely at optimum cost.

Table 1.3.2: Steps involved in Implementing Business Process Automation

Step 1: Define why we plan to implement BPA?	• The answer to this question will provide justification for implementing BPA.
Step 2: Understand the rules/ regulation under which it needs to comply with?	• The underlying issue is that any BPA created needs to comply with applicable laws and regulations.
Step 3: Document the process, we wish to automate.	• The current processes which are planned to be automated need to be correctly and completely documented at this step.
Step 4: Define the objectives/goals to be achieved by implementing BPA.	• This enables the developer and user to understand the reasons for going for BPA. The goals need to be precise and clear.
Step 5: Engage the business process consultant.	• Once the entity has been able to define the above, the entity needs to appoint an expert, who can implement it for the entity.
Step 6: Calculate the RoI for project.	• The answer to this question can be used for convincing top management to say 'yes' to the BPA exercise.
Step 7: Development of BPA.	• Once the top management grant their approval, the right business solution has to be procured and implemented or developed and implemented covering the necessary BPA.
Step 8: Testing the BPA.	• Before making the process live, the BPA solutions should be fully tested.

(iv) Step 4: Define the objectives/goals to be achieved by implementing BPA

Once the above steps have been completed, entity needs to determine the key objectives of the process improvement activities. When determining goals, remember that goals need to be **SMART**:

♦ **Specific:** Clearly defined,

- **Measurable:** Easily quantifiable in monetary terms,
- **Attainable:** Achievable through best efforts,
- **Relevant:** Entity must be in need of these, and
- **Timely:** Achieved within a given time frame.

For example,

Case 1: For vendor's offering early payment discounts, entity needs to consider:

- How much could be saved if they were taken advantage of, and if the entity has got the cash flow to do so?
- Vendor priority can be created based on above calculations, for who gets paid sooner rather than later.

Case 2: To determine the average invoice aging per customer. Entity can decide to reduce the average from 75 days to 60 days. This alone can dramatically improve cash flow.

(v) Step 5: Engage the business process consultant

This is again a critical step to achieve BPA. To decide as to which company/ consultant to partner with, depends upon the following:

- Objectivity of consultant in understanding/evaluating entity situation.
- Does the consultant have experience with entity business process?
- Is the consultant experienced in resolving critical business issues?
- Whether the consultant can recommend and implementing a combination of hardware, software and services as appropriate to meeting enterprise BPA requirements?
- Does the consultant have the required expertise to clearly articulate the business value of every aspect of the proposed solution?

(vi) Step 6: Calculate the RoI for project

The right stakeholders need to be engaged and involved to ensure that the benefits of BPA are clearly communicated and implementation becomes successful. Hence, the required business process owners have to be convinced so as to justify the benefits of BPA and get approval from senior management. A lot of meticulous effort would be required to convince the senior management about need to implement the right solution for BPA. The right business case has to be made covering technical and financial feasibility so as to justify and get approval for implementing the BPA. The best way to convince would be to generate a proposition that communicates to the stakeholders that BPA shall lead to not only cost savings for the enterprise but also improves efficiency and effectiveness of service offerings.

Some of the methods for justification of a BPA proposal may include:

- Cost Savings, being clearly computed and demonstrated.
- How BPA could lead to reduction in required manpower leading to no new recruits need to be hired and how existing employees can be re-deployed or used for further expansion.
- Savings in employee salary by not having to replace those due to attrition.
- The cost of space regained from paper, file cabinets, reduced.
- Eliminating fines to be paid by entity due to delays being avoided.
- Reducing the cost of audits and lawsuits.
- Taking advantage of early payment discounts and eliminating duplicate payments.
- Ensuring complete documentation for all new accounts.
- New revenue generation opportunities.
- Collecting accounts receivable faster and improving cash flow.
- Building business by providing superior levels of customer service.
- Charging for instant access to records (e.g. public information, student transcripts, medical records)

The above can be very well presented to justify the proposal and convince management to go ahead with the project of BPA implementation as required for the enterprise.

(vii) Step 7: Developing the BPA

Once the requirements have been document, ROI has been computed and top management approval to go ahead has been received, the consultant develops the requisite BPA. The developed BPA needs to meet the objectives for which the same is being developed.

(viii) Step 8: Testing the BPA

Once developed, it is important to test the new process to determine how well it works and identify where additional “exception processing” steps need to be included. The process of testing is an iterative process, the objective being to remove all problems during this phase.

Testing allows room for improvements prior to the official launch of the new process, increases user adoption and decreases resistance to change. Documenting the final version of the process will help to capture all of this hard work, thinking and experience which can be used to train new people.

1.3.4 Case studies on Business Processes Automation

Case 1: Automation of purchase order generation process in a manufacturing entity

Various steps of automation are given as follows:

Step 1: Define why we plan to go for a BPA?

The entity has been facing the problem of non-availability of critical raw material items which is leading to production stoppages and delay in delivery. Delay in delivery has already costed company in terms of losing customer and sales.

Step 2: Understand the rules / regulation under which needs to comply with?

The item is not covered by regulation, regarding quantity to be ordered or stored. To keep cost at minimum entity has calculated economic order quantity for which orders are placed.

Step 3: Document the process, we wish to automate.

The present process is manual where the orders are received by purchase department from stores department. Stores department generates the order based on manual stock register, based on item's re-order levels. The levels were decided five years back and stores records are not updated timely.

Step 4: Define the objectives/goals to be achieved by implementing BPA.

The objective behind the present exercise is to ensure that there are no production losses due to non-availability of critical items of inventory. This shall automatically ensure timely delivery of goods to customer.

Step 5: Engage the business process consultant.

ABC Limited, a consultant of repute, has been engaged for the same. The consultant has prior experience and knowledge about entity's business.

Step 6: Calculate the ROI for project.

The opportunity loss for the project comes to around ₹ 100/- lakhs per year. The cost of implementing the whole BPA shall be around ₹ 50/- lakhs. It is expected that the opportunity loss after BPA shall reduce to ₹ 50 lakhs in year one, ₹ 25/- lakhs in later years for the next five years. For students:

- Is the project worth going ahead?
- What is the RoI, based on three years' data?
- What is the payback period?

Step 7: Developing the BPA.

Once the top management says yes, the consultant develops the necessary BPA. The BPA is to generate purchase orders as soon as an item of inventory reaches its re-order level. To ensure accuracy, all data in the new system need to be checked and validated before being put the same into system:

- Item's inventory was physically counted before uploading to new system.
- Item's re-order levels were recalculated.
- All items issued for consumption were timely updated in system.
- All Purchase orders automatically generated are made available to Purchase manager at end of day for authorizations.

Step 8: Testing the BPA.

Before making the process live, it should be thoroughly tested.

Case 2: Automation of Employee Attendance

Various steps of automation are given as follows:

Step 1: Define why we plan to go for a BPA?

The system of recording of attendance being followed is not generating confidence in employees about the accuracy. There have been complaints that salary payouts are not as per actual attendance. It has also created friction and differences between employees, as some feels that other employees have been paid more for their salary has not been deducted for being absent.

Step 2: Understand the rules/regulation under which needs to comply with?

Number of regulations is applicable to employee attendance including Factories Act 1948, Payment of Wages Act 1936, State laws, etc. This is a compliance requirement and hence, any BPA needs to cater to these requirements.

Step 3: Document the process, we wish to automate.

The present system includes an attendance register and a register at the security gate. Employees are expected to put their signatures in attendance registers. The register at the gate is maintained by security staff, to mark when an employee has entered. There is always a dispute regarding the time when an employee has entered and what has been marked in the security register. The company policy specifies that an employee coming late by 30 minutes for two days in a month shall have a ½ day salary deduction. There is over-writing in attendance register, leading to heated arguments between human resource department staff and employees. As the time taken to arrive at the correct attendance is large, there is a delay in preparation of salary. The same has already led to penal action against company by labor department of the state.

Step 4: Define the objectives/goals to be achieved implementing BPA.

The objective for implementing BPA, being:

- Correct recording of attendance.
- Timely compilation of monthly attendance so that salary can be calculated and distributed on a timely basis.
- To ensure compliance with statutes.

Step 5: Engage the business process consultant.

XYZ Limited a consultant of repute has been engaged for the same. The consultant has prior experience and knowledge about entity's business.

Step 6: Calculate the RoI for project.

The BPA may provide tangible benefits in the form of reduced penalties and intangible benefits which may include:

- Better employee motivation and morale,
- Reduced difference between employees,
- More focus on work rather than salary, and
- Improved productivity.

Step 7: Developing the BPA.

Implementing BPA includes would result in the following:

- All employees would be given electronic identity cards.

- The cards would contain details about employees.
- The attendance system would work in the following manner:
  - Software with card reading machine would be installed at the entry gate.
  - Whenever an employee enters or leaves the company, he/she needs to put the card in front of machine.
  - The card reading machine would be linked to the software which would record the attendance of the employee.
  - At the end of month, the software would print attendance reports employee-wise. These reports would also point out how many days an employee has reported late in the month.
  - Based on this report monthly attendance is put in the system to generate the monthly salary.

Step 8: Testing the BPA.

Before making the process live, it should be thoroughly tested.

The above illustrations are of entities, which have gone for business process automation. There are thousands of processes across the world for which entity have gone for BPA and reaped numerous benefits. These include:

- Tracking movement of goods,
- Sales order processing,
- Customer services departments,
- Inventory management,
- Employee Management System, and
- Asset tracking systems.

1.4 RISKS AND ITS MANAGEMENT

1.4.1 Introduction

Risk is any event that may result in a significant deviation from a planned objective resulting in an unwanted negative consequence. The planned objective could be any aspect of an enterprise's strategic, financial, regulatory and operational processes, products or services. The degree of risk associated with an event is determined by the likelihood (uncertainty, probability) of the event occurring, the consequences (impact) if the event were to occur and it's timing.

1.4.2 Sources of Risk

The most important step in risk management process is to identify the sources of risk, the areas from where risks can occur. This will give information about the possible threats, vulnerabilities and accordingly appropriate risk mitigation strategy can be adapted. Some of the common sources of risk are Commercial and Legal Relationships, Economic Circumstances, Human Behavior, Natural Events, Political Circumstances, Technology and Technical Issues, Management Activities and Controls, and Individual Activities.

Broadly, risk has the following characteristics:

- ***Potential loss that exists as the result of threat/vulnerability process;***
- ***Uncertainty of loss expressed in terms of probability of such loss; and***
- ***The probability/likelihood that a threat agent mounting a specific attack against a particular system.***

1.4.3 Types of Risks

The risks broadly can be categorized as follows:

A. *Business Risks*: *Businesses face all kinds of risks related from serious loss of profits to even bankruptcy and are discussed below:*

- ***Strategic Risk*: *These are the risks that would prevent an organization from accomplishing its objectives (meeting its goals). Examples include risks related to strategy, political, economic, regulatory, and global market conditions; also, could include reputation risk, leadership risk, brand risk, and changing customer needs***
- ***Financial Risk*: *Risk that could result in a negative financial impact to the organization (waste or loss of assets). Examples include risks from volatility in foreign currencies, interest rates, and commodities; credit risk, liquidity risk, and market risk.***
- ***Regulatory (Compliance) Risk*: *Risk that could expose the organization to fines and penalties from a regulatory agency due to non-compliance with laws and regulations. Examples include Violation of laws or regulations governing areas such as environmental, employee health and safety, protection of personal data in accordance with global data protection requirements and local tax or statutory laws.***

- ***Operational Risk*: Risk that could prevent the organization from operating in the most effective and efficient manner or be disruptive to other operations. Examples include risks related to the organization's human resources, business processes, technology, business continuity, channel effectiveness, customer satisfaction, health and safety, environment, product/service failure, efficiency, capacity, and change integration.**

- ***Hazard Risk*: Risks that are insurable, such as natural disasters; various insurable liabilities; impairment of physical assets; terrorism etc.**

- ***Residual Risk*: Any risk remaining even after the counter measures are analyzed and implemented is called Residual Risk. An organization's management of risk should consider these two areas: *Acceptance of residual risk* and *Selection of safeguards*. Even when safeguards are applied, there is probably going to be some residual risk. The risk can be minimized, but it can seldom be eliminated. Residual risk must be kept at a minimal, acceptable level. As long as it is kept at an acceptable level, (i.e. the likelihood of the event occurring or the severity of the consequence is sufficiently reduced) the risk can be managed**

B. Technology Risk: The dependence on technology in BPA for most of the key business processes has led to various challenges. As Technology is taking new forms and transforming as well, the business processes and standards adapted by enterprises 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 challenge 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 Technology architecture used for services could include multiple digital platforms and is quite complex. Hence, this requires the personnel to have knowledge about requisite technology skills or the management of the 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.

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

(v) **Dependence on vendors due to outsourcing of IT services:** In a systems environment, the organization requires staff with specialized domain skills to manage IT deployed. 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 application 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):** Organizations may 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. 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 system environment provides access to customers anytime, anywhere using internet. Hence, information system which was earlier accessible only within and to the employees 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.

(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 unauthorized to commit frauds. For example: extracting information about passwords from 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 system 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 organization, senior management should be involved in directing how technology is deployed in 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.

C. ***Data related risks:*** These include Physical access of data and Electronic access of data. (these are well explained in Chapter 3)

1.4.4 Risk Management and Related Terms

Various terminologies relating to risk management are given as follows:

***Risk Management:* Risk Management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. Risk management involves identifying, measuring, and minimizing uncertain events affecting resources.**

***Asset:* Asset can be defined as something of value to the organization; e.g., information in electronic or physical form, software systems, employees. Irrespective the nature of the assets themselves, they all have one or more of the following characteristics:**

- ***They are recognized to be of value to the organization.***
- ***They are not easily replaceable without cost, skill, time, resources or a combination.***
- ***They form a part of the organization's corporate identity, without which, the organization may be threatened.***
- ***Their data classification would normally be Proprietary, Highly confidential or even Top Secret.***

It is the purpose of Information Security Personnel to identify the threats against the risks and the associated potential damage to, and the safeguarding of Information Assets.

Vulnerability: ***Vulnerability is the weakness in the system safeguards that exposes the system to threats. It may be a weakness in information system/s, cryptographic system (security systems), or other components (e.g. system security procedures, hardware design, internal controls) that could be exploited by a threat. Vulnerabilities potentially "allow" a threat to harm or exploit the system. For example, vulnerability could be a poor access control method allowing dishonest employees (the threat) to exploit the system to adjust their own records. Some examples of vulnerabilities are given as follows:***

- ***Leaving the front door unlocked makes the house vulnerable to unwanted visitors.***
- ***Short passwords (less than 6 characters) make the automated information system vulnerable to password cracking or guessing routines.***

Missing safeguards often determine the level of vulnerability. Determining vulnerabilities involves a security evaluation of the system including inspection of safeguards, testing, and penetration analysis.

Normally, vulnerability is a state in a computing system (or set of systems), which must have at least one condition, out of the following:

- ***'Allows an attacker to execute commands as another user' or***
- ***'Allows an attacker to access data that is contrary to the specified access restrictions for that data' or***
- ***'Allows an attacker to pose as another entity' or***
- ***'Allows an attacker to conduct a denial of service'.***

Threat: ***Any entity, circumstance, or event with the potential to harm the software system or component through its unauthorized access, destruction, modification, and/or denial of service is called a Threat. It is an action, event or condition where there is a compromise in the system, its quality and ability to inflict harm to the organization. Threat has capability to attack on a system with intent to harm. It is often to start threat modeling with a list of known threats and vulnerabilities found in similar systems. Every system has a data, which is considered as a fuel to drive a system, data is nothing but assets. Assets and threats are closely correlated. A threat cannot exist without a target asset. Threats are typically prevented by applying some sort of protection to assets.***

<u>Exposure:</u> An exposure is the extent of loss the enterprise has to face when a risk materializes. It is not just the immediate impact, but the real harm that occurs in the long run. For example - loss of business, failure to perform the system's mission, loss of reputation, violation of privacy and loss of resources etc.

<u>Likelihood:</u> Likelihood of the threat occurring is the estimation of the probability that the threat will succeed in achieving an undesirable event. The presence, tenacity and strengths of threats, as well as the effectiveness of safeguards must be considered while assessing the likelihood of the threat occurring.

<u>Attack</u>: An attack is an attempt to gain unauthorized access to the system's services or to compromise the system's dependability. In software terms, an attack is a malicious intentional fault, usually an external fault that has the intent of exploiting vulnerability in the targeted software or system.

Basically, it is a set of actions designed to compromise <u>CIA (Confidentiality, Integrity or Availability)</u>, or any other desired feature of an information system. Simply, it is the act of trying to defeat Information Systems (IS) safeguards. The type of attack and its degree of success determines the consequence of the attack.

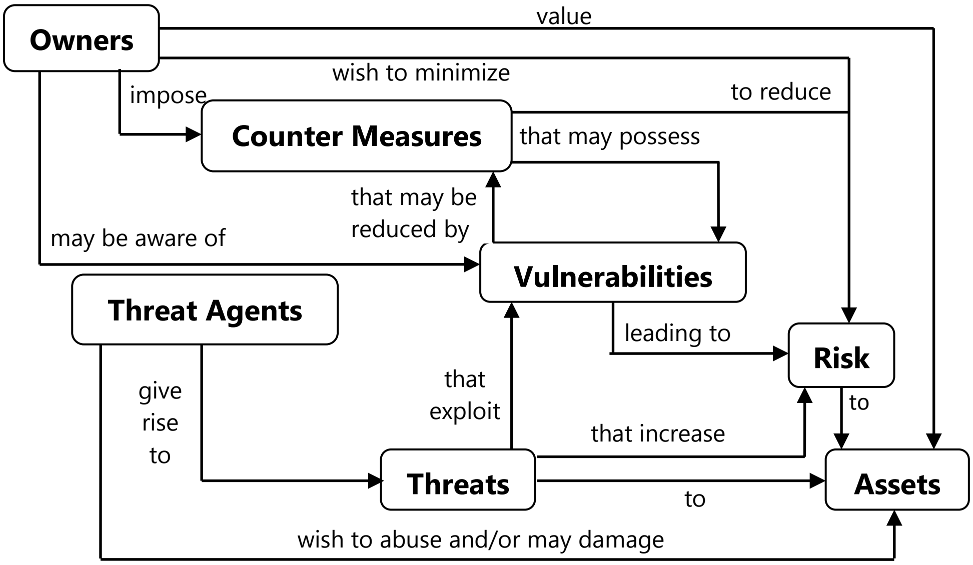


Fig. 1.4.1: Risk and Related Terms

<u>Counter Measure:</u> An action, device, procedure, technique or other measure that reduces the vulnerability of a component or system is referred as Counter

Measure. For example, well known threat 'spoofing the user identity', has two countermeasures:

- ***Strong authentication protocols to validate users; and***
- ***Passwords should not be stored in configuration files instead some secure mechanism should be used.***

Similarly, for other vulnerabilities, different countermeasures may be used.

The relationship and different activities among these terms may be understood by the Fig. 1.4.1.

Concludingly, Risk can be defined as the potential harm caused if a threat exploits a particular vulnerability to cause damage to an asset, and Risk Analysis is defined as the process of identifying security risks and determining their magnitude and impact on an organization. Risk Assessment includes the following:

- ***Identification of threats and vulnerabilities in the system;***
- ***Potential impact or magnitude of harm that a loss of CIA, would have on enterprise operations or enterprise assets, should an identified vulnerability be exploited by a threat; and***

New technology provides the potential for dramatically enhanced business performance, improved and demonstrated information risk reduction and security measures. Technology can also add real value to the organization by contributing to interactions with the trading partners, closer customer relations, improved competitive advantage and protected reputation.

1.4.5 Risk Management Strategies

Effective risk management begins with a clear understanding of an enterprise'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:

When risks are identified, and analyzed, it is not always appropriate to implement controls to counter them. Some risks may be minor, and it may not be cost effective to implement expensive control processes for them. Risk management strategy is explained and illustrated below:

- ***Tolerate/Accept the risk*. One of the primary functions of management is managing risk. Some risks may be considered minor because their impact and probability of occurrence is low. In this case, consciously accepting the risk as a cost of doing business is appropriate, as well as periodically reviewing the risk to ensure its impact remains low.**
- ***Terminate/Eliminate the risk.* It is possible for a risk to be associated with the use of a technology, supplier, or vendor. The risk can be eliminated by replacing the technology with more robust products and by seeking more capable suppliers and vendors.**
- ***Transfer/Share the risk.* Risk mitigation approaches can be shared with trading partners and suppliers. A good example is outsourcing infrastructure management. In such a case, the supplier mitigates the risks associated with managing the IT infrastructure by being more capable and having access to more highly skilled staff than the primary organization. Risk also may be mitigated by transferring the cost of realized risk to an insurance provider.**
- ***Treat/mitigate the risk.* Where other options have been eliminated, suitable controls must be devised and implemented to prevent the risk from manifesting itself or to minimize its effects.**
- ***Turn back.* Where the probability or impact of the risk is very low, then management may decide to ignore the risk.**

1.5 CONTROLS

Control is defined as policies, procedures, practices and organization structure that are designed to provide reasonable assurance that business objectives are achieved and undesired events are prevented or detected and corrected.

Based on the mode of implementation, these controls can be Manual, Automated or Semi-Automated (partially manual and partially automated). The objective of a control is to mitigate the risk.

Example - Purchase to Pay: Given below is a simple example of controls for the Purchase to Pay cycle, which is broken down to four main components as shown in the Fig. 1.5.1.

- **Purchases:** When an employee working in a specific department (i.e., marketing, operations, sales, etc.) wants to purchase something required for carrying out the job, he/she will submit a Purchase Requisition (PR) to a manager for approval. Based on the approved PR, a Purchase Order (PO) is raised. The PO may be raised manually and then input into the computer system or raised directly by the computer system.

- **Goods Receipt:** The PO is then sent to the vendor, who will deliver the goods as per the specifications mentioned in the PO. When the goods are received at the warehouse, the receiving staff checks the delivery note, PO number etc. and acknowledges the receipt of the material. Quantity and quality are checked and any unfit items are rejected and sent back to the vendor. A Goods Receipt Note (GRN) is raised indicating the quantity received. The GRN may be raised manually and then input into the computer system or raised directly by computer system.

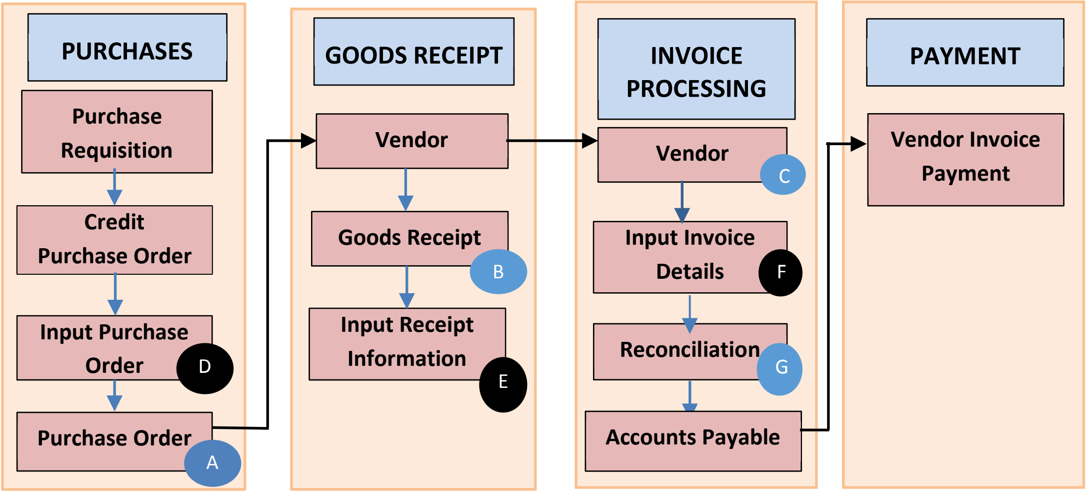


Fig. 1.5.1: Purchase Cycle – Sample Controls

- **Invoice Processing:** The vendor sends the invoice to the accounts payable department who will input the details into the computer system. The vendor invoice is checked with the PO to ensure that only the goods ordered have been invoiced and at the negotiated price. Further the vendor invoice is checked with the GRN to ensure that the quantity ordered has been received.

- **Payment:** If there is no mismatch between the PO, GRN and vendor invoice; the payment is released to the vendor based on the credit period negotiated with the vendor.

Based on the mode of implementation, these controls can be Manual, Automated or Semi-Automated (partially manual and partially automated). The objective of a control is to mitigate the risk.

- **Manual Control:** Manually verify that the goods ordered in PO (A) are received (B) in good quality and the vendor invoice (C) reflects the quantity and price that are as per the PO (A).
- **Automated Control:** The above verification is done automatically by the computer system by comparing (D), (E) & (F) and exceptions highlighted.
- **Semi-Automated Control:** Verification of Goods Receipt (E) with PO (D) could be automated but the vendor invoice matching could be done manually in a reconciliation process (G).

1.5.1 Importance of IT Controls

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 provide 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.

1.5.2 Applying IT Controls

It is important for an organization to identify controls as per policy, procedures and its structure and configure it within IT software as used in the organization.

There are different options for implementing controls as per risk management strategy. For example, the way banking is done in a 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.

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) Information Technology General Controls (ITGC)

ITGC also known as Infrastructure Controls pervade across different layers of IT environment and information systems 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 organization structure with key demarcation of duties for different personnel within IT department and to ensure that there are no Segregation of Duties (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 center.

- **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 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.
- **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.
- **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 is 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.

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. These are designed to ensure completeness, accuracy, authorization and validity of data capture and transaction processing. For example: In banking, 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).

1.5.3 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 organization 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.
- ♦ Heightened security awareness on the part of the users and a security conscious culture.

1.5.4 Framework of Internal Control as per Standards on Auditing

SA 315 defines the system of Internal Control as "the process designed, implemented and maintained by those charged with governance, management and other personnel to provide reasonable assurance about the achievement of an entity's objectives regarding reliability of financial reporting, effectiveness and efficiency of operations, safeguarding of assets, and compliance with applicable laws and regulations.

An Internal Control System -

- facilitates the effectiveness and efficiency of operations.
- helps ensure the reliability of internal and external financial reporting.
- assists compliance with applicable laws and regulations.
- helps safeguarding the assets of the entity.

The five components of any internal control as they relate to a financial statement audit are explained below.

I. Control Environment

The Control Environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The Board of Directors and Senior Management establish the tone at the top regarding the importance of internal control, including expected standards of conduct. Management reinforces expectations at the various levels of the organization. The control environment comprises the integrity and ethical values of the organization; the parameters enabling the board of directors to carry out its governance responsibilities; the organizational structure and assignment of authority and responsibility; the process for attracting, developing, and retaining competent individuals; and the rigor around performance measures, incentives, and rewards to drive accountability for performance. The resulting control environment has a pervasive impact on the overall system of internal control.

II. Risk Assessment

Every entity faces a variety of risks from external and internal resources. Risk may be defined as the possibility that an event will occur and adversely affect the achievement of objectives. **Risk Assessment** involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives. Risks to the achievement of these objectives from across the entity are considered relative to established risk tolerances.

Thus, Risk Assessment forms the basis for determining how risks will be managed. A precondition to risk assessment is the establishment of objectives, linked at different levels of the entity. Management specifies objectives within categories of operations, reporting, and compliance with sufficient clarity to be able to identify and assess risks to those objectives. Risk assessment also requires management to consider the impact of possible changes in the external environment and within its own business model that may render internal control ineffective.

III. Control Activities

Control Activities are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the entity, at various stages within business processes, and over the technology environment. They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations and business performance reviews.

Broadly, the control activities include the elements that operate to ensure transactions are authorized, duties are segregated, adequate documents and records are maintained, assets and records are safeguarded, and independent checks on performance and valuation of records. Internal auditors are also concerned with administrative controls to achieve effectiveness and efficiency objectives. Control activities must be developed to manage, mitigate, and reduce the risks associated with each business process. It is unrealistic to expect to eliminate risks completely.

IV. Information and Communication

Information is necessary for the entity to carry out internal control responsibilities in support of the achievement of its objectives. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of other components of internal control. **Communication** is the continual, iterative process of providing, sharing, and obtaining necessary information. Internal communication is how information is disseminated throughout the enterprise, flowing up, down, and across the entity. It enables personnel to receive a clear message from senior management that control responsibilities should be taken seriously. External communication is two-fold: it enables inbound communication of relevant external information and provides information to external parties in response to requirements and expectations.

V. Monitoring of Controls

Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to affect the principles within each component is present and functioning. Ongoing evaluations built into business processes at different levels of the entity, provide timely information. Separate evaluations, conducted periodically, will vary in scope and frequency depending on assessment of risks, effectiveness of ongoing evaluations, and other management considerations. Findings are evaluated against management's criteria and deficiencies are communicated to management and the Board of Directors as appropriate.

1.5.5 Limitations of Internal Control System

Internal control, no matter how effective, can provide an entity with only reasonable assurance and not absolute assurance about achieving the entity's operational, financial reporting and compliance objectives. Internal control systems are subject to certain inherent limitations, such as:

- Management's consideration that the cost of an internal control does not exceed the expected benefits to be derived.
- The fact that most internal controls do not tend to be directed at transactions of unusual nature. The potential for human error, such as, due to carelessness, distraction, mistakes of judgement and misunderstanding of instructions.
- The possibility of circumvention of internal controls through collusion with employees or with parties outside the entity.
- The possibility that a person responsible for exercising an internal control could abuse that responsibility, for example, a member of management overriding an internal control.
- Manipulations by management with respect to transactions or estimates and judgements required in the preparation of financial statements.

1.6 ENTERPRISE RISK MANAGEMENT

In implementing controls, it is important to adapt a holistic and comprehensive approach. Hence, ideally it should consider the overall business objectives, processes, organization structure, technology deployed and the risk appetite. Based on this, overall risk management strategy has to be adapted, which should be designed and promoted by the top management and implemented at all levels of enterprise operations as required in an integrated manner. Regulations require enterprises to adapt a risk management strategy, which is appropriate for the enterprise. Hence, the type of controls implemented in information systems in an enterprise would depend on this risk management strategy. **The Sarbanes Oxley Act (SOX)** in the US, which focuses on the implementation and review of internal controls as relating to financial audit, highlights the importance of evaluating the risks, security and controls as related to financial statements. In an IT environment, it is important to understand whether the relevant IT controls are implemented.

How controls are implemented would be dependent on the overall risk management strategy and risk appetite of the management.

Enterprise Risk Management (ERM) may be defined as a process, affected by an entity's Board of Directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

The underlying premise of Enterprise Risk Management (ERM) is that every entity, whether for profit, not-for-profit, or a governmental body, exists to provide value for its stakeholders. All entities face uncertainty, and the challenge for management is to determine how much uncertainty the entity is prepared to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value. ERM provides a framework for management to effectively deal with uncertainty and associated risk and opportunity and thereby enhance its capacity to build value.

It is important for management to ensure that the enterprise risk management strategy considers implementation of information and its associated risks while formulating IT security and controls as relevant. IT security and controls are a sub-set of the overall enterprise risk management strategy and encompass all aspects of activities and operations of the enterprise.

ERM in business includes the methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives. ERM is a common framework applied by business management and other personnel to identify potential events that may affect the enterprise manage the associated risks and opportunities and provide reasonable assurance that an enterprise's objectives will be achieved.

1.6.1 Benefits of Enterprise Risk Management

No entity operates in a risk-free environment and ERM does not create such an environment. Rather, it enables management to operate more effectively in environments filled with risks. ERM provides enhanced capability to do the following:

- **Align risk appetite and strategy:** Risk appetite is the degree of risk, on a broad-based level that an enterprise (any type of entity) is willing to accept in pursuit of its goals. Management considers the entity's risk appetite first in evaluating strategic alternatives, then in setting objectives aligned with the selected strategy and in developing mechanisms to manage the related risks.

- **Link growth, risk and return:** Entities accept risk as part of value creation and preservation, and they expect return commensurate with the risk. ERM provides an enhanced ability to identify and assess risks, and establish acceptable levels of risk relative to growth and return objectives.
- **Enhance risk response decisions:** ERM provides the rigor to identify and select among alternative risk responses – risk avoidance, reduction, sharing and acceptance. ERM provides methodologies and techniques for making these decisions.
- **Minimize operational surprises and losses:** Entities have enhanced capability to identify potential events, assess risk and establish responses, thereby reducing the occurrence of surprises and related costs or losses.
- **Identify and manage cross-enterprise risks:** Every entity faces a myriad of risks affecting different parts of the enterprise. Management needs to not only manage individual risks, but also understand interrelated impacts.
- **Provide integrated responses to multiple risks:** Business processes carry many inherent risks, and ERM enables integrated solutions for managing the risks.
- **Seize opportunities:** Management considers potential events, rather than just risks, and by considering a full range of events, management gains an understanding of how certain events represent opportunities.
- **Rationalize capital:** More robust information on an entity's total risk allows management to more effectively assess overall capital needs and improve capital allocation.

1.6.2 Enterprise Risk Management Framework

ERM provides a framework for risk management which typically involves identifying events or circumstances relevant to the organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress. By identifying and pro-actively addressing risks and opportunities, business enterprises protect and create value for their stakeholders, including owners, employees, customers, regulators, and society overall.

ERM framework consists of eight interrelated components that are derived from the way management runs a business, and are integrated with the management process. These components are as follows:

(i) **Internal Environment:** The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate. Management sets a philosophy regarding risk and establishes a risk appetite. The internal environment sets the foundation for how risk and control are viewed and addressed by an entity's people. The core of any business is its people – their individual attributes, including integrity, ethical values and competence – and the environment in which they operate. They are the engine that drives the entity and the foundation on which everything rests.

(ii) **Objective Setting:** Objectives should be set before management can identify events potentially affecting their achievement. ERM ensures that management has a process in place to set objectives and that the chosen objectives support and align with the entity's mission/vision and are consistent with the entity's risk appetite.

(iii) **Event Identification:** Potential events that might have an impact on the entity should be identified. Event identification includes identifying factors – internal and external – that influence how potential events may affect strategy implementation and achievement of objectives. It includes distinguishing between potential events that represent risks, those representing opportunities and those that may be both. Opportunities are channeled back to management's strategy or objective-setting processes. Management identifies inter-relationships between potential events and may categorize events to create and reinforce a common risk language across the entity and form a basis for considering events from a portfolio perspective.

(iv) **Risk Assessment:** Identified risks are analyzed to form a basis for determining how they should be managed. Risks are associated with related objectives that may be affected. Risks are assessed on both an inherent and a residual basis, and the assessment considers both risk likelihood and impact. A range of possible results may be associated with a potential event, and management needs to consider them together.

(v) **Risk Response:** Management selects an approach or set of actions to align assessed risks with the entity's risk tolerance and risk appetite, in the context of the strategy and objectives. Personnel identify and evaluate possible responses to risks, including avoiding, accepting, reducing and sharing risk.

(vi) **Control Activities:** Policies and procedures are established and executed to help ensure that the risk responses that management selected, are effectively carried out.

(vii) Information and Communication: Relevant information is identified, captured and communicated in a form and time frame that enable people to carry out their responsibilities. Information is needed at all levels of an entity for identifying, assessing and responding to risk. Effective communication also should occur in a broader sense, flowing down, across and up the entity. Personnel need to receive clear communications regarding their role and responsibilities.

(viii) Monitoring: The entire ERM process should be monitored, and modifications made as necessary. In this way, the system can react dynamically, changing as conditions warrant. Monitoring is accomplished through ongoing management activities, separate evaluations of the ERM processes or a combination of the both.

1.7 DIAGRAMMATIC REPRESENTATION OF BUSINESS PROCESSES

1.7.1 Introduction to Flowcharts

Flowcharts are used in designing and documenting simple processes or programs. Like other types of diagrams, they help visualize what is going on and thereby help understand a process, and perhaps also find flaws, bottlenecks, and other less-obvious features within it. There are many different types of flowcharts, and each type has its own repertoire of boxes and notational conventions. The two most common types of boxes in a flowchart are as follows:

- a processing step, usually called **activity,** and denoted as a **rectangular box**.
- a **decision** usually denoted as a **diamond**.

A **Flowchart** is described as “cross-functional” when the page is divided into different swimlanes describing the control of different organizational units. A symbol appearing in a particular “lane” is within the control of that organizational unit. This technique allows the author to locate the responsibility for performing an action or deciding correctly, showing the responsibility of each organizational unit for different parts of a single process.

I. Flowcharting Symbols

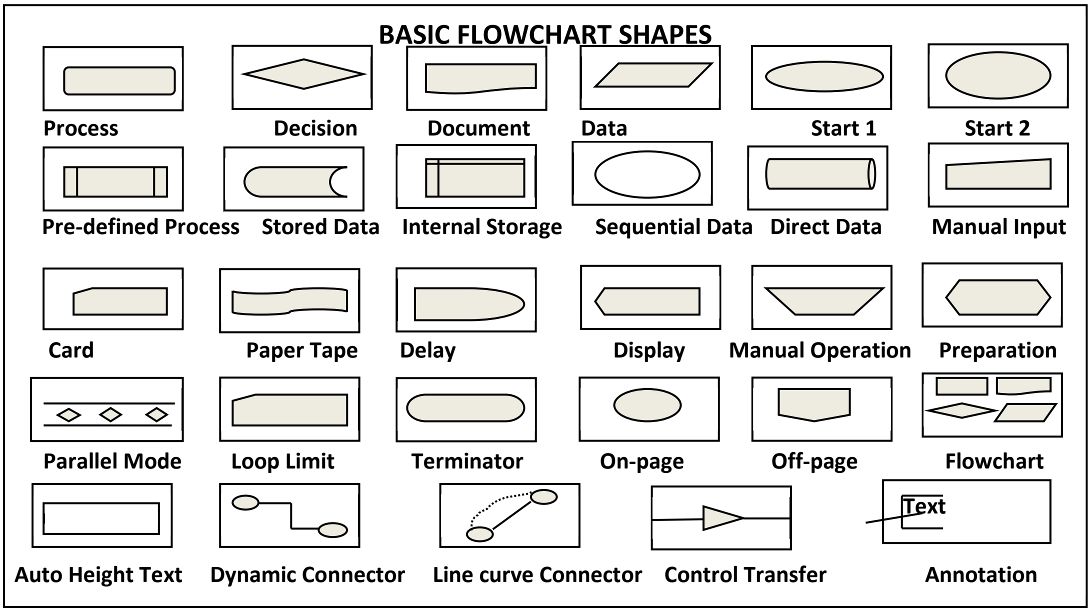


Fig. 1.7.1: Flowcharting Symbols

II. Steps for creating flowcharts for business processes

- Identify the business process that is to be documented with a flowchart and establish the overall goal of the business process.
- Based on inputs from the business process, owner obtains a complete understanding of the process flow.
- Prepare an initial rough diagram and discuss with the business process owner to confirm your understanding of the processes.
- Obtain additional information about the business process from the people involved in each step, such as end users, stakeholders, administrative assistants and department heads. During this phase, you may find that some employees do not follow certain processes or some processes are redundant. This should be highlighted so that corrective steps can be taken by the management.
- Identify the activities in each process step and who is responsible for each activity.
- Identify the starting point of the process. The starting point of a business process should be what triggers the process to action. In other words, it is the input that the business seeks to convert into an output. Starting points generally fall into one of several categories:

  - **External events:** These include the initiation of a transaction or a transmitted alert from another business system. For example, creation of a purchase order in a computer system or a sales order alerting a production system that a product should be manufactured due to lack of available stock.
  - **Content arrival:** For content management systems, the starting point might be the arrival of a new document or other form of content.
  - **Human intervention:** This includes customer complaints and other human intervention within or outside of the business.

- ♦ Separate the different steps in the process. Identify each individual step in the process and how it is connected to the other steps. On the most general level, you will have events (steps that require no action by the business), activities (performed by the business in response to input), and decision gateways (splits in the process where the path of the process is decided by some qualifier). Between these objects, there are connectors, which can be either be solid arrows (activity flow), or dashed (message/information flow).
- ♦ In traditional **Business Process Modeling Notation (BPMN)**, the steps are represented by different shapes depending on their function. For example, we would use steps such as "customer order" (an event), "process order" (an activity), "Check credit" (an action), "Credit?" (a decision gateway that leads to one of two other actions, depending on a "yes" or "no" determination), and so on.
- ♦ Clarify who or what performs each step. To make the process as clear as possible, you should determine which part of the business completes each step. Different parts of the process may be completed by the accounting department, customer service, or order fulfillment, for example. Alternately, for a small business, these steps may be completed by specific individuals. In BPMN, the associated person or department for each activity is either denoted by a designator next to the step or by a horizontal division or "lanes" in the flow chart that shows which part of the business performs each step, i.e., person or department.

Fig. 1.7.2 is a very simple flowchart which represents a process that happens in our daily life.

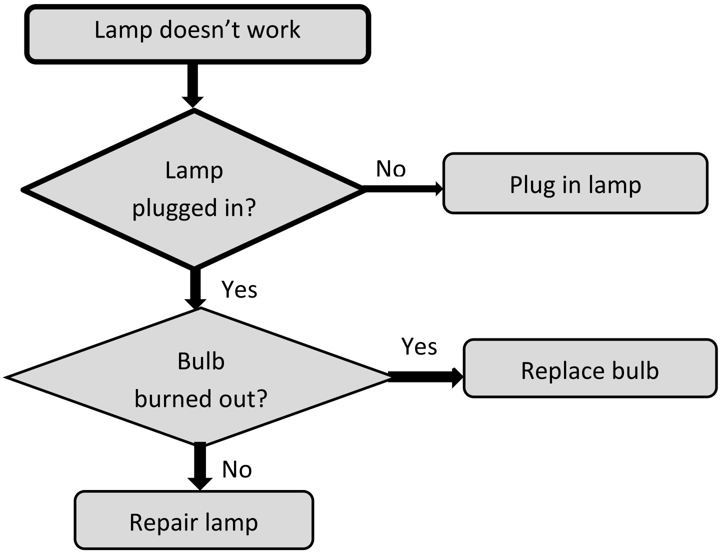


Fig. 1.7.2: Simple Flowchart

III. Advantages of Flowcharts

(i) Quicker grasp of relationships - The relationship between various elements of the application program/business process must be identified. Flowchart can help depict a lengthy procedure more easily than by describing it by means of written notes.

(ii) Effective Analysis - The flowchart becomes a blue print of a system that can be broken down into detailed parts for study. Problems may be identified and new approaches may be suggested by flowcharts.

(iii) Communication - Flowcharts aid in communicating the facts of a business problem to those whose skills are needed for arriving at the solution.

(iv) Documentation - Flowcharts serve as a good documentation which aid greatly in future program conversions. In the event of staff changes, they serve as training function by helping new employees in understanding the existing programs.

(v) Efficient coding - Flowcharts act as a guide during the system analysis and program preparation phase. Instructions coded in a programming language may be checked against the flowchart to ensure that no steps are omitted.

(vi) Program Debugging - Flowcharts serve as an important tool during program debugging. They help in detecting, locating and removing mistakes.

(vii) Efficient program maintenance - The maintenance of operating programs is facilitated by flowcharts. The charts help the programmer to concentrate attention on that part of the information flow which is to be modified.

(viii) Identifying Responsibilities - Specific business processes can be clearly identified to functional departments thereby establishing responsibility of the process owner.

(ix) Establishing Controls - Business process conflicts and risks can be easily identified for recommending suitable controls.

IV. Limitations of Flowchart

(i) Complex logic – Flowchart becomes complex and clumsy where the problem logic is complex. The essentials of what is done can easily be lost in the technical details of how it is done.

(ii) Modification – If modifications to a flowchart are required, it may require complete re-drawing.

(iii) Reproduction – Reproduction of flowcharts is often a problem because the symbols used in flowcharts cannot be typed.

(iv) Link between conditions and actions – Sometimes it becomes difficult to establish the linkage between various conditions and the actions to be taken there upon for a condition.

(v) Standardization – Program flowcharts, although easy to follow, are not such a natural way of expressing procedures as writing in English, nor are they easily translated into Programming language.

Example 1: Draw a Flowchart for finding the sum of first 100 odd numbers.

Solution 1: The flowchart is drawn as Fig. 1.7.3 and is explained step by step below. The step numbers are shown in the flowchart in circles and as such are not a part of the flowchart but only a referencing device.

Our purpose is to find the sum of the series 1, 3, 5, 7, 9.....(100 terms). The student can verify that the 100th term would be 199. We propose to set A = 1 and then go on incrementing it by 2 so that it holds the various terms of the series in turn. B is an accumulator in the sense that A is added to B whenever A is incremented. Thus, B will hold:

1

1 + 3 = 4

4 + 5 = 9,

9 + 7 = 16, etc. in turn.

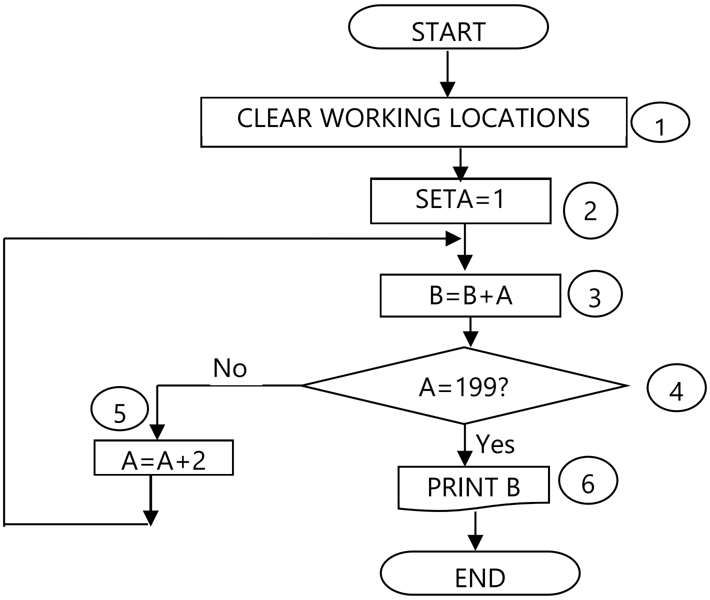


Fig. 1.7.3: Flowchart for addition of first 100 odd numbers

Step 1 - All working locations are set at zero. This is necessary because if they are holding some data of the previous program, that data is liable to corrupt the result of the flowchart.

Step 2 - A is set at 1 so that subsequently by incrementing it successively by 2, we get the wanted odd terms: 1,3,5,7 etc.

Step 3 - A is poured into B i.e., added to B. B being 0 at the moment and A being 1, B becomes 0 + 1 = 1.

Step 4 - Step 4 poses a question. "Has A become 199?" if not, go to step 5, we shall increment A by 2. So, that although at the moment A is 1, it will be made 3 in step 5, and so on. Then go back to step 3 by forming loop.

Since we must stop at the 100th term which is equal to 199, Thus, A is repeatedly incremented in step 5 and added to B in step 3. In other words, B holds the cumulative sum up to the latest terms held in A.

When A has become 199 that means the necessary computations have been carried out so that in step 6 the result is printed.

Example 2

An E-commerce site has the following cash back offers.

(i) If purchase mode is via website, an initial discount of 10% is given on bill amount.

(ii) If purchase mode is via phone app, an initial discount of 20% is given on bill amount.

(iii) If done via any other purchase mode, the customer is not eligible for any discount.

Every purchase eligible to discount is given 10 reward points.

(a) If the reward points are between 100 and 200 points, the customer is eligible for a further 30% discount on the bill amount after initial discount.

(b) If the reward points exceed 200 points, the customer is eligible for a further 40% discount on the bill amount after initial discount.

Taking purchase mode, bill amount and number of purchases as input; draw a flowchart to calculate and display the total reward points and total bill amount payable by the customer after all the discount calculation.

Solution 2

Let us define the variables first:

PM: Purchase Mode	**BA:** Bill Amount	**TBA:** Total Bill Amount
NOP: Number of Purchases	**TRP:** Total Reward Points	**IN_DISC:** Initial Discount

ET_DISC: Extra Discount on purchases eligible to Initial Discount

N: Counter (to track the no. of purchases)

Refer Fig. 1.7.4 the desired flowchart.

<u>Example 3</u>

A bank has 500 employees. The salary paid to each employee is sum of his Basic Pay (BP), Dearness Allowance (DA) and House Rent Allowance (HRA). For computing HRA, bank has classified his employees into three classes A, B and C. The HRA for each class is computed at the rate of 30%, 20% and 10% of the BP Pay respectively. The DA is computed at a flat rate of 60% of the Basic Pay. Draw a flow chart to determine percentage of employee falling in the each of following salary slabs:

(i) Above ₹30,000

(ii) ₹15,001 to ₹30,000

(iii) ₹8,001 to ₹15,000

(iv) Less than or equal to ₹8,000

Solution 3

The required flowchart is given in Fig. 1.7.5:

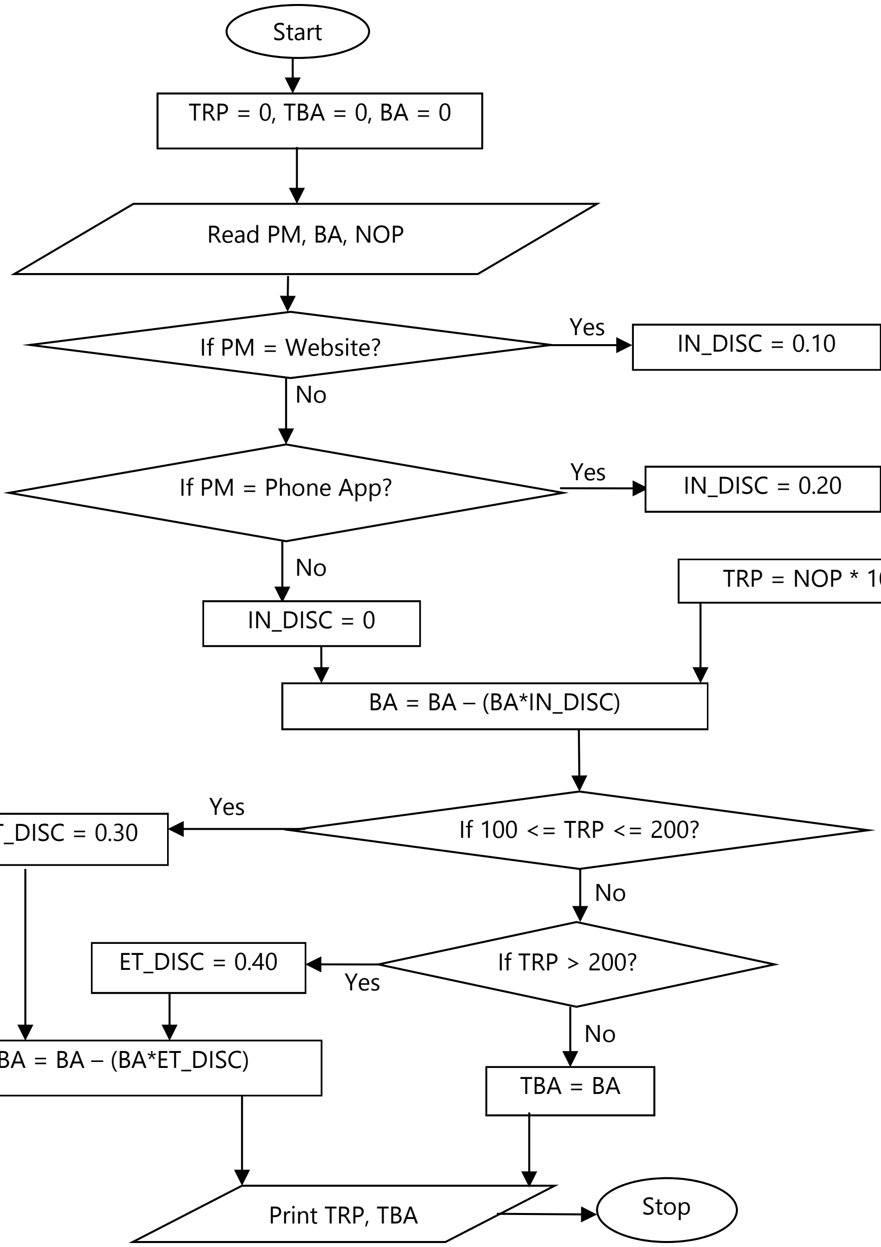


Fig. 1.7.4: Flowchart for Example 2

Solution 3 (Ctd.)

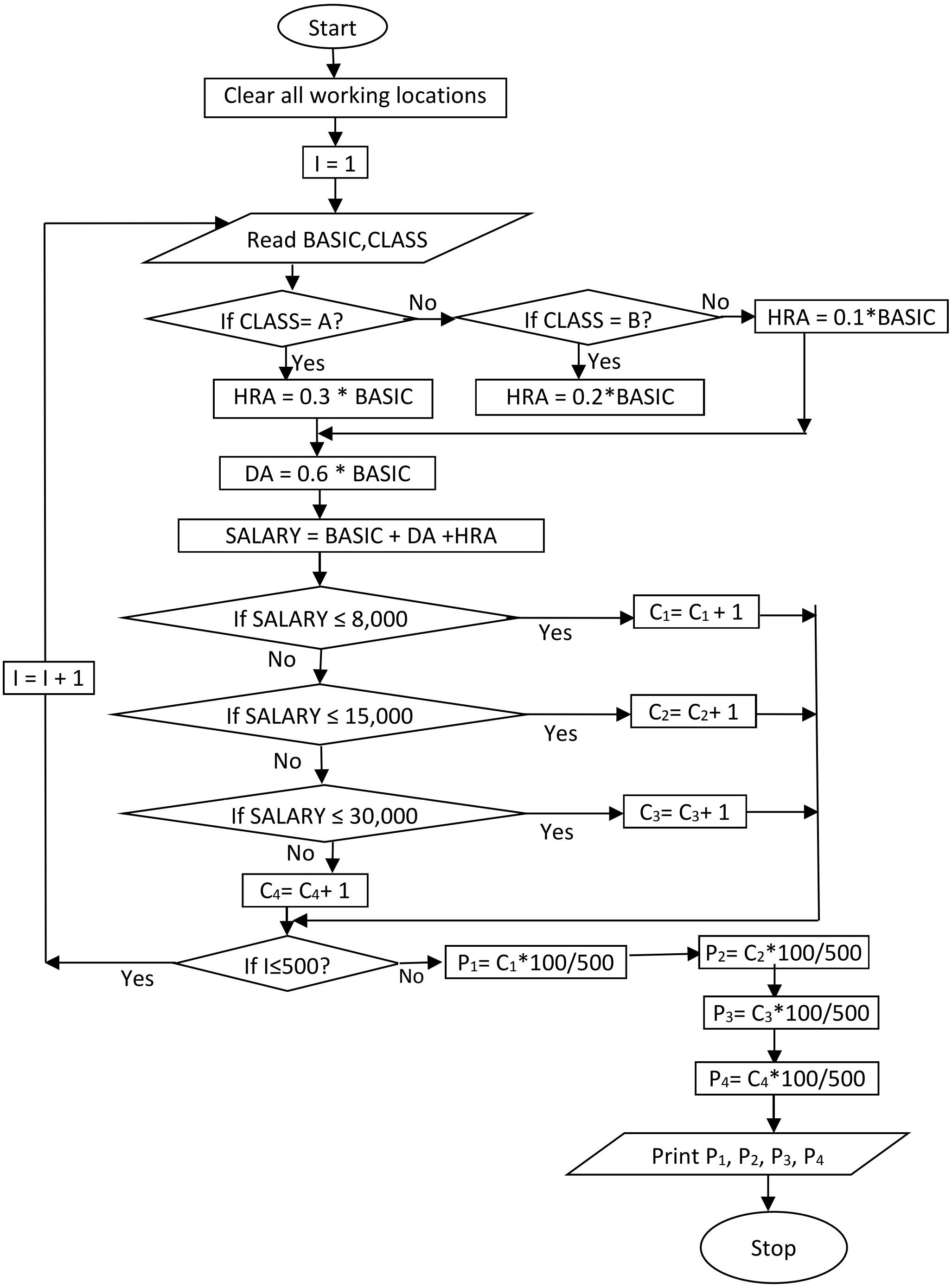


Fig. 1.7.5: Flowchart for Example 3

Abbreviations used in the above flowchart are as follows:

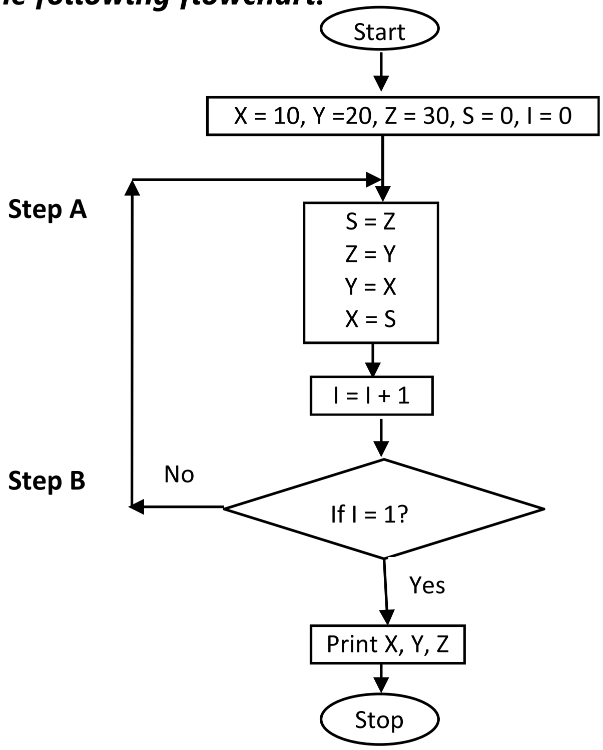
P_1, P_2, P_3 and P_4: Percentage of employees falling in salary slab (salary <= 8,000); salary slab (8,001 <= salary <= 15,000); salary slab (15,001 <= salary <= 30,000) and salary slab (salary >= 30,000) respectively;

C_1, C_2, C_3 and C_4: are the number of employees falling in salary slab (salary<=8,000); salary slab (8,001 <= salary <=15,000); salary slab (15,001 <= salary <= 30,000) and salary slab (salary >= 30,000) respectively;

I: Count of number of employees

<u>Example 4</u>

Consider the following flowchart:



(a) What is the output of the flowchart?

(b) In Step B, put I = 3 in place of I = 1; what will be the output then?

(c) In Step B, put I = 6 in place of I = 1; what will be the output then?

(d) In the given flowchart; replace I = 0 by I = 1 at Step A, what will be the output?

Solution 4

Working of the Flowchart

Initial Values	Sequence of Steps	Output 1	Output 2	Output 3	Output 4	Output5	Output6
I = 0							
S = 0	S = Z	S = 30	S = 20	S = 10	S = 30	S = 20	S = 10
Z = 30	Z = Y	Z = 20	Z = 10	Z = 30	Z = 20	Z = 10	Z = 30
Y = 20	Y = X	Y = 10	Y = 30	Y = 20	Y = 10	Y = 30	Y = 20
X = 10	X = S	X = 30	X = 20	X = 10	X = 30	X = 20	X = 10
I = 0	I = I + 1	I = 1	I = 2	I = 3	I = 4	I = 5	I = 6
		Answer (a)		Answer (b)			Answer (c)

(a) ***X = 30, Y = 10, Z = 20***

(b) ***For I = 3; X = 10, Y = 20, Z = 30***

(c) ***For I = 6; X = 10, Y = 20, Z = 30***

(d) ***For I = 1 at Step A; the flowchart will enter an Infinite Loop as the condition I = 1 will never be true.***

Example 5

A company is selling three types of products namely A, B and C to two different types of customers viz. dealers and retailers. To promote the sales, the company of offering the following discounts. Draw a flowchart to calculate the discount for the above policy

(i) ***10% discount is allowed on product A, irrespective of the category of customers and the value of order.***

(ii) ***On product B, 8% discount is allowed to retailers and 12% discount to dealers, irrespective of the value of order.***

(iii) ***On product C, 15% discount is allowed to retailers irrespective of the value of order and 20% discount to dealers if the value of order is minimum of ₹ 10,000.***

Solution 5

The required flowchart is given in Fig. 1.7.6:

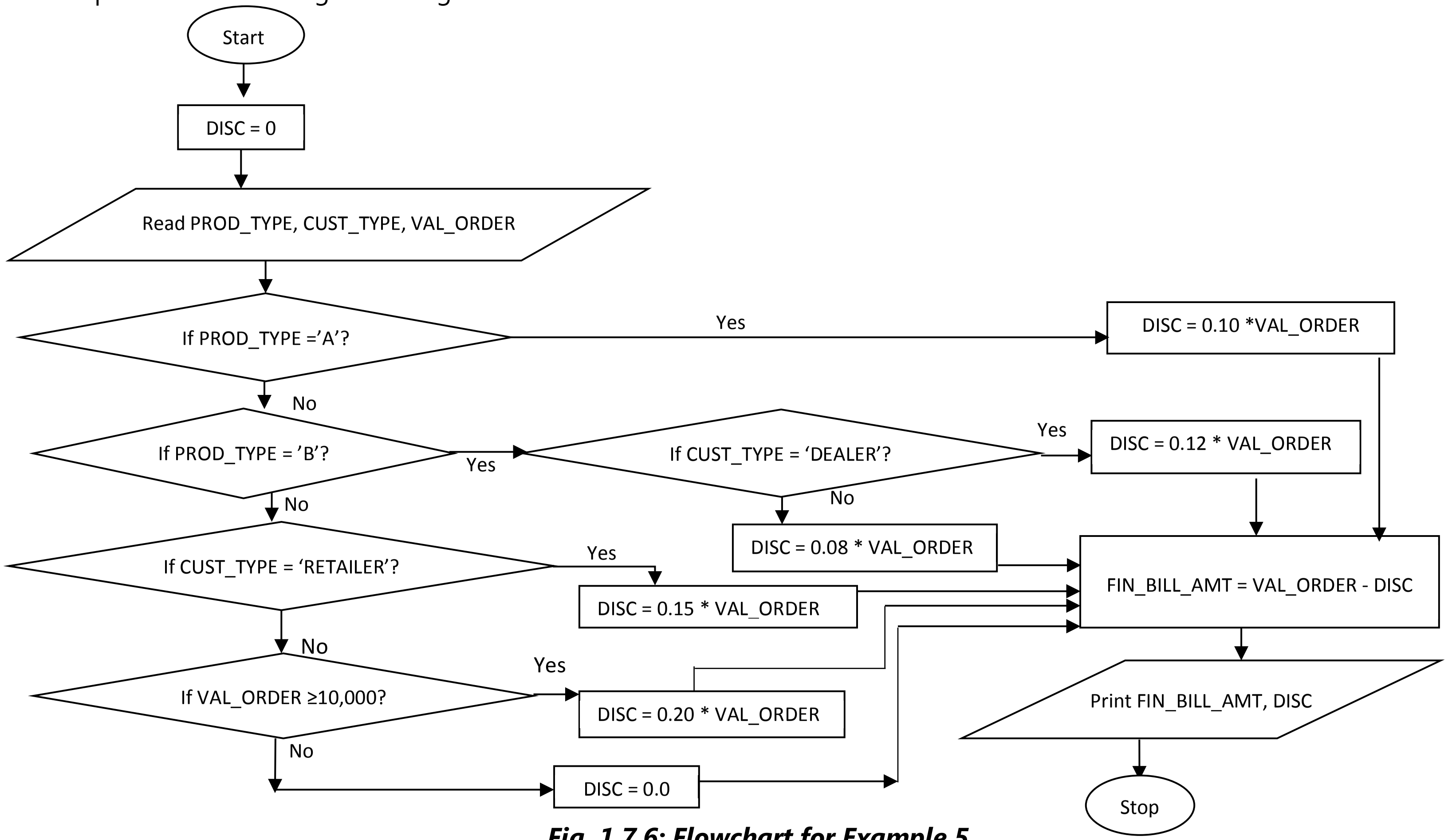


Fig. 1.7.6: Flowchart for Example 5

1.7.2 Introduction to Data Flow Diagrams (DFDs)

The Fig. 1.7.7 depicts a simple business process (traditional method) flow. The limitation of this diagram is that processes are not identified to functional departments.

Data Flow Diagrams – Processes are identified to functional departments. Data Flow Diagrams (DFD) show the flow of data or information from one place to another. DFDs describe the processes showing how these processes link together through data stores and how the processes relate to the users and the outside world.

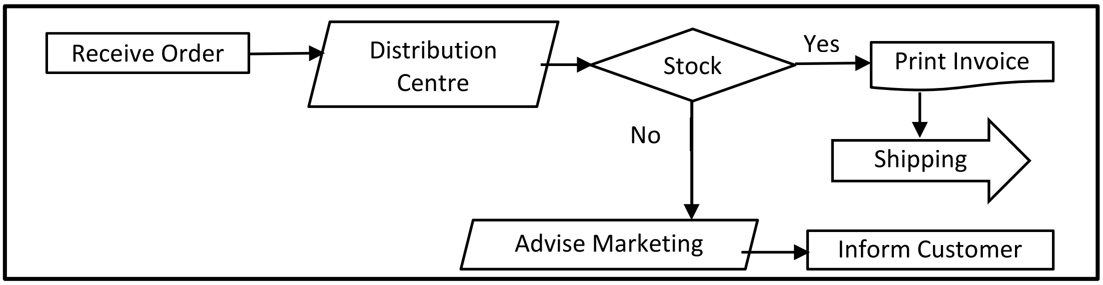


Fig. 1.7.7: Simple Flow chart of Sales (Example)

In the simple DFD shown in Fig. 1.7.8, please note that the processes are specifically identified to the function using "swimlanes". Each lane represents a specific department where the business process owner can be identified. The business process owner is responsible for ensuring that adequate controls are implemented, to mitigate any perceived business process risks.

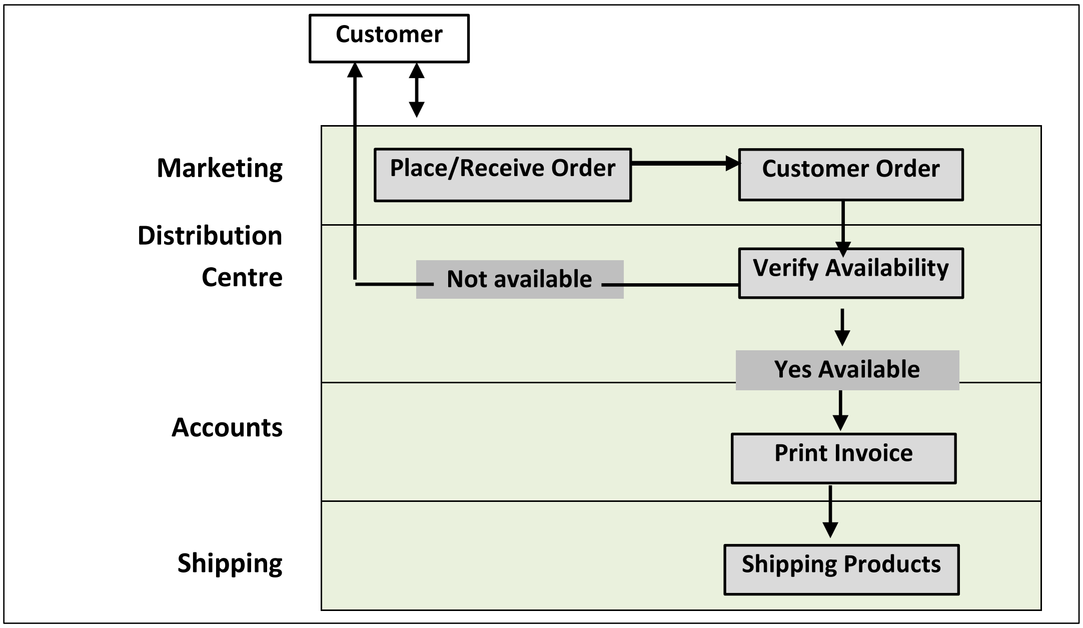


Fig. 1.7.8: Process flow of Sales (Example)

DFD basically provides an overview of:

- What data a system processes;
- What transformations are performed;
- What data are stored;
- What results are produced and where they flow.

It is mainly used by technical staff for graphically communicating between systems analysts and programmers.

Main symbols used in DFD (Refer Fig. 1.7.9)

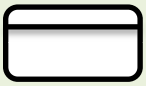
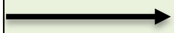
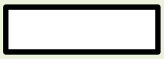
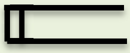
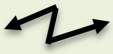
	**Process**	Step-by-step instructions are followed that transform inputs into outputs (a computer or person or both doing the work)
	**Data flow**	Data flowing from place to place, such as an input or output to a process
	**External Agent**	The source or destination of data outside the system.
	**Data Store**	Data at rest, being stored for later use. Usually corresponds to a data entity on an entity-relationship diagram.
	**Real-time link**	Communication back and forth between an external agent and a process as the process is executing (e.g. credit card verification).

Fig. 1.7.9: DFD Symbols

Data Flow Diagrams – Processes are identified to functional departments.

Given below in Fig. 1.7.10 is a simple scenario depicting a book borrowed from a library being returned and the fine calculated, due to delay.

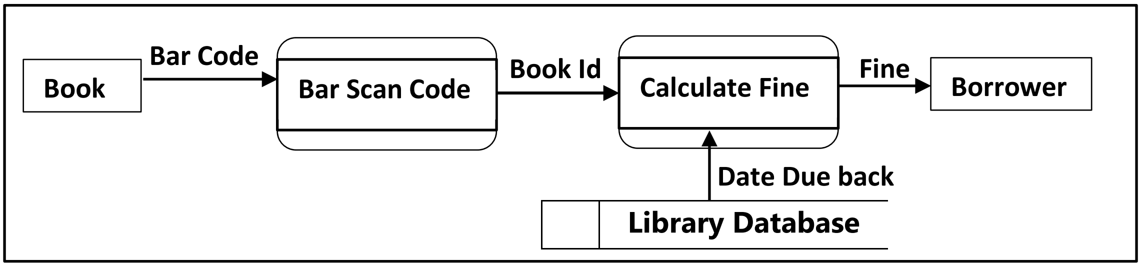


Fig. 1.7.10: Simple DFD (Example)

- The book is represented as an external entity and the input is the bar code.
- The process is the scanning of the bar code and giving an output of the Book ID.
- The next process calculates the fine based on accessing the "library database" and establishing the "due back" date.
- Finally, the fine is communicated to the borrower who is also shown as an external entity.

1.7.3 Diagrammatic Representation of Specific Business Processes

I. Customer Order Fulfilment (Refer Fig. 1.7.11)

- The process starts with the customer placing an order and the sales department creating a sales order.
- The sales order goes through the Credit & Invoicing process to check credit (an activity) is it OK? (a decision gateway).

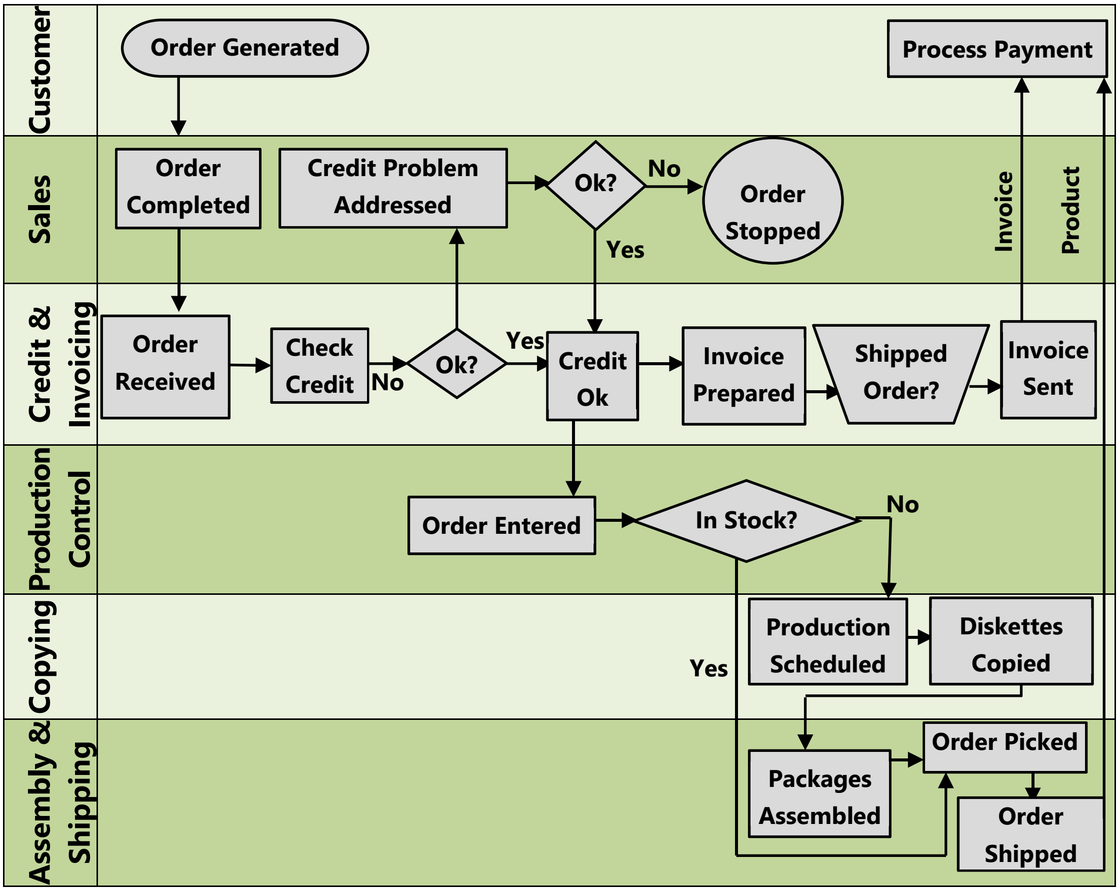


Fig. 1.7.11: Customer Order Fulfilment (Example)

- ♦ If the customer's credit check is not OK, you would move to the step "credit problem addressed" (an activity), followed by a decision "OK?". If, "No" the order will be stopped.
- ♦ If the customer's "credit check" response is "yes", and if stock is available, an invoice is prepared, goods shipped and an invoice is sent to the customer. If the stock is not available, the order is passed to "production control" for manufacture and then shipped to customer with the invoice.
- ♦ The process ends with the payment being received from customer.

II. Order to Cash (Refer Fig. 1.7.12)

Fig. 1.7.12 indicates the different sub processes within the main processes in the Order to Cash cycle. It should be noted that this is only a simple example to illustrate the concept. However, in large enterprises the main processes, sub processes and activities could be much more.

(i) Sales and Marketing (SM)

- Advertises and markets the company's products and books sales orders from customers.

(ii) Order Fulfilment

- Receives orders from SM.
- Checks inventory to establish availability of the product. If the product is available in stock, transportation is arranged and the product is sent to the customer.

(iii) Manufacturing

- If the product is not available in stock, this information is sent to the manufacturing department so that the product is manufactured and subsequently sent to the customer.

(iv) Receivables

- The invoice is created, sent to the customer, payment received and the invoice closed.
- It should be noted that under each sub process, there could be many activities. For example:
  - o **Main Process** - Order Fulfilment
  - o **Sub Process –**Receive Orders
  - o **Other Activities –**Check correctness and validity of information in order, enter order in computer system, check credit worthiness of customer, check credit limit, obtain approval for any discrepancy etc.

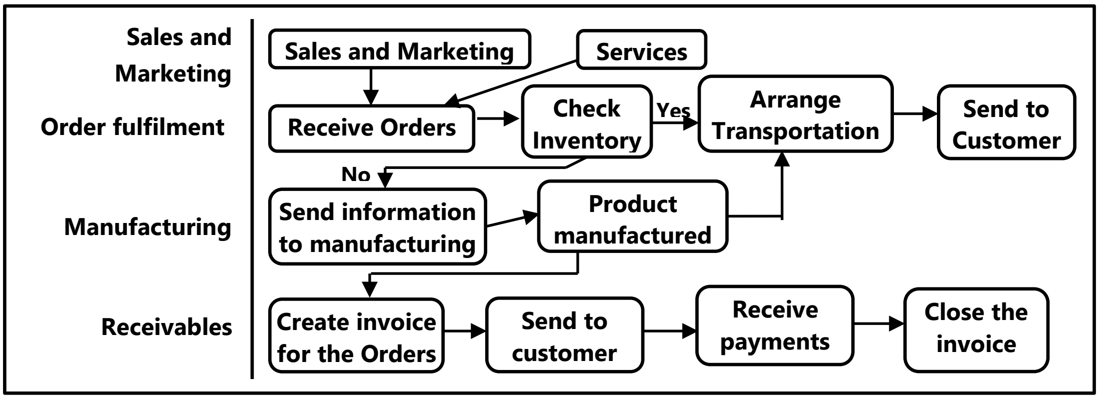


Fig. 1.7.12: Order to Cash (Example)

III. Procure to Pay (Refer Fig. 1.7.13)

The **Purchase to Pay/Procure to Pay** process in Fig. 1.7.13 indicates the different processes identified specifically to department/entity through "swimlanes" so that the responsibilities are clearly defined. Let's understand flow from the perspective of each department/entity.

(i) User Department

- A user in an enterprise may require some material or service. Based on the need and justification, the user raises a Purchase Request (PR) to the Procurement department.

(ii) Procurement Department (PD)

- PD receives the PR and prioritizes the request based on the need and urgency of the user.
- It is then the responsibility of the PD to find the best source of supply, for the specific material/service. PD will then request the potential vendors to submit their quotes, based on which negotiations on price, quality and payment terms, will take place.
- The Purchase Order (PO) will then be released to the selected vendor.

(iii) Vendor

- The vendor receives the PO and carries out his own internal checks.
- Matches the PO with the quotation sent and in the event of any discrepancy will seek clarification from the enterprise.
- If there are no discrepancies, the vendor will raise an internal sales order within the enterprise.
- The material is then shipped to the address indicated in the PO.
- The Vendor Invoice (VI) is sent to the Accounts Payable department, based on the address indicated in the PO.

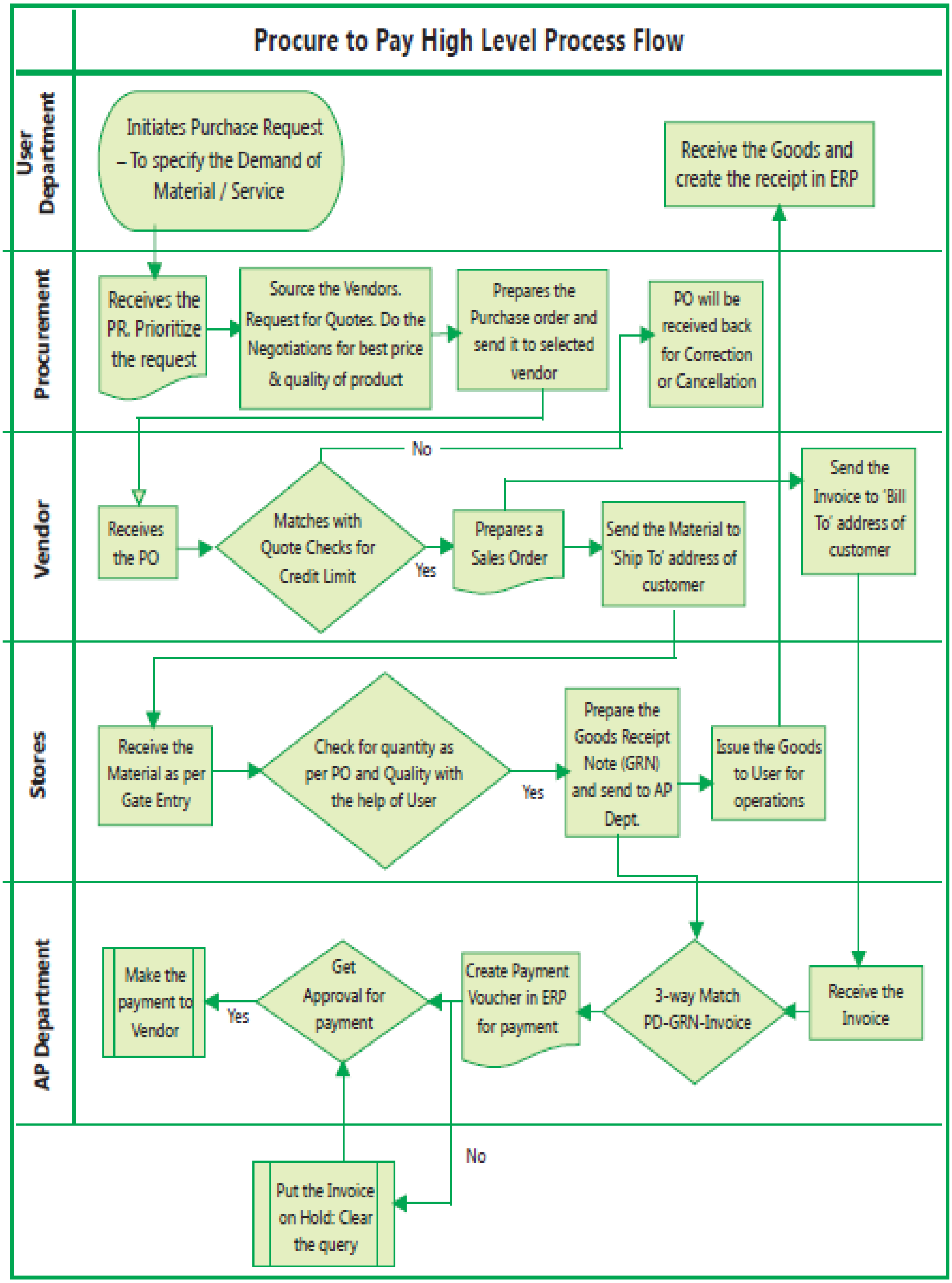

Procure to Pay High Level Process Flow
User Department
Procurement
Vendor
Stores
AP Department
Initiates Purchase Request – To specify the Demand of Material / Service
Receive the Goods and create the receipt in ERP
Receives the PR. Prioritize the request
Source the Vendors. Request for Quotes. Do the Negotiations for best price & quality of product
Prepares the Purchase order and send it to selected vendor
PO will be received back for Correction or Cancellation
No
Receives the PO
Matches with Quote Checks for Credit Limit
Yes
Prepares a Sales Order
Send the Material to 'Ship To' address of customer
Send the Invoice to 'Bill To' address of customer
Receive the Material as per Gate Entry
Check for quantity as per PO and Quality with the help of User
Yes
Prepare the Goods Receipt Note (GRN) and send to AP Dept.
Issue the Goods to User for operations
Make the payment to Vendor
Yes
Get Approval for payment
Create Payment Voucher in ERP for payment
3-way Match PD-GRN-Invoice
Receive the Invoice
No
Put the Invoice on Hold: Clear the query

Fig. 1.7.13: Procure to Pay (Example)

(iv) Stores

- Receives the material.
- Checks the quantity received with the PO and quality with the users. If there is any discrepancy the vendor is immediately informed.
- The Goods Received Note (GRN) is prepared based on the actual receipt of material and the stores stock updated. The GRN is then sent to the Accounts Payable department for processing the payment.
- A Material Issue Note is created and the material is sent to the concerned user.

(v) Accounts Payable (AP)

AP will do a "3-way match" of PO/GRN/VI. This is to ensure that the price, quantity and terms indicated in the VI matches with the PO and the quantity received in the PO matches with the GRN quantity. This check establishes that what has been ordered has been delivered.

♦ If there is no discrepancy, the payment voucher is prepared for payment and the necessary approvals obtained.

♦ If there is a discrepancy, the VI is put "on hold" for further clarification and subsequently processed.

♦ Finally, the payment is made to the vendor.

1.8 RISKS AND CONTROLS FOR SPECIFIC BUSINESS PROCESSES

1.8.1 Business Processes - Risks and Controls

Suitable controls should be implemented to meet the requirements of the control objectives. These controls can be manual, automated or semi-automated provided the risk is mitigated. Based on the scenario, the controls can be **Preventive**, **Detective** or **Corrective**. Preventive controls prevent risks from actualizing. Detective controls detect the risks as they arise. Corrective controls facilitate correction. In computer systems, controls should be checked at three levels, namely **Configuration**, **Masters** and **Transaction** level.

1. Configuration

Configuration refers to the way a software system is set up. Configuration is the methodical process of defining options that are provided. When any software is installed, values for various parameters should be set up (configured) as per policies and business process work flow and business process rules of the enterprise. The various modules of the enterprise such as Purchase, Sales, Inventory, Finance, User Access etc. must be configured. Configuration will define how software will function and what menu options are displayed. Some examples of configuration are given below:

- Mapping of accounts to front end transactions like purchase and sales
- Control on parameters: Creation of Customer Type, Vendor Type, year-end process
- User activation and deactivation
- User Access & privileges - Configuration & its management
- Password Management

2. Masters

Masters refer to the way various parameters are set up for all modules of software, like Purchase, Sales, Inventory, and Finance etc. These drives how the software will process relevant transactions. The masters are set up first time during installation and these are changed whenever the business process rules or parameters are changed. Examples are Vendor Master, Customer Master, Material Master, Accounts Master, Employee Master etc. Any changes to these data have to be authorized by appropriate personnel and these are logged and captured in exception reports. The way masters are set up will drive the way software will process transactions of that type. For example: The Customer Master will have the credit limit of the customer. When an invoice is raised, the system will check against the approved credit limit and if the amount invoiced is within the credit limit, the invoice will be created if not the invoice will be put on "credit hold" till proper approvals are obtained.

Some examples of masters are given here:

- **Vendor Master:** Credit period, vendor bank account details, etc.
- **Customer Master:** Credit limit, Bill to address, Ship to address, etc.
- **Material Master:** Material type, Material description, Unit of measure, etc.
- **Employee Master:** Employee name, designation, salary details, etc.

3. Transactions

Transactions refer to the actual transactions entered through menus and functions in the application software, through which all transactions for specific modules are initiated, authorized or approved. For example: Sales transactions, Purchase transactions, Stock transfer transactions, Journal entries and Payment transactions.

Implementation or review of specific business process can be done from risk or control perspective. In case of risk perspective, we need to consider each of the key sub-processes or activities performed in a business process and look at existing and related control objectives and existing controls and the residual risks after application of controls. The residual risk should be knowingly accepted by the management.

If we review this from a control objective perspective, then for each key sub-process or activity, we will consider what is sought to be achieved by implementing controls and then evaluate whether risks are mitigated by controls which are implemented at present and what are the residual risks and whether there is need to complement/add more controls.

Given below are some examples of risks and controls for a few business processes. The checklist provided below are illustrative. It is not necessary that all the sub-processes/activities given below are applicable for all enterprises. However, they are provided to build an understanding of the sub-processes, risk and related controls and control objectives. This list can be practically used for implementation/evaluation of risk/controls of business processes detailed below. However, it should be customized specifically as per the nature of business processes and how these are implemented in the enterprise. The checklist given below is categorized into Configuration, Masters and Transactions.

1.8.2 Procure to Pay (P2P) – Risks and Controls

Procure to Pay (Purchase to Pay or P2P) is the process of obtaining and managing the raw materials needed for manufacturing a product or providing a service. It involves the transactional flow of data that is sent to a supplier as well as the data that surrounds the fulfillment of the actual order and payment for the product or service. Using automation, it should be possible to have a seamless procure to pay process covering the complete life-cycle from point of order to payment.

Masters

Table 1.8.1: Risks and Control Objectives (Masters-P2P)

Risk	Control Objective
Unauthorized changes to supplier master file.	Only valid changes are made to the supplier master file.
All valid changes to the supplier master file are not input and processed.	All valid changes to the supplier master file are input and processed.

Changes to the supplier master file are not correct.	Changes to the supplier master file are accurate.
Changes to the supplier master file are delayed and not processed in a timely manner.	Changes to the supplier master file are processed in a timely manner.
Supplier master file data is not up to date.	Supplier master file data remain up to date.
System access to maintain vendor masters has not been restricted to the authorized users.	System access to maintain vendor masters has been restricted to the authorized users.

Transactions

Table 1.8.2: Risks and Control Objectives (Transactions-P2P)

Risk	Control Objective
Unauthorized purchase requisitions are ordered.	Purchase orders are placed only for approved requisitions.
Purchase orders are not entered correctly in the system.	Purchase orders are accurately entered.
Purchase orders issued are not input and processed.	All purchase orders issued are input and processed.
Amounts are posted in accounts payable for goods or services not received.	Amounts posted to accounts payable represent goods or services received.
Amounts posted to accounts payable are not properly calculated and recorded.	Accounts payable amounts are accurately calculated and recorded.
Amounts for goods or services received are not input and processed in accounts payable.	All amounts for goods or services received are input and processed to accounts payable.
Amounts for goods or services received are recorded in the wrong period.	Amounts for goods or services received are recorded in the appropriate period.
Accounts payable amounts are adjusted based on unacceptable reasons.	Accounts payable are adjusted only for valid reasons.
Credit notes and other adjustments are not accurately calculated and recorded.	Credit notes and other adjustments are accurately calculated and recorded.

All valid credit notes and other adjustments related to accounts payable are not input and processed.	All valid credit notes and other adjustments related to accounts payable are input and processed.
Credit notes and other adjustments are recorded in the wrong period.	Credit notes and other adjustments are recorded in the appropriate period.
Disbursements are made for goods and services that have not been received.	Disbursements are made only for goods and services received.
Disbursements are distributed to unauthorized suppliers.	Disbursements are distributed to the appropriate suppliers.
Disbursements are not accurately calculated and recorded.	Disbursements are accurately calculated and recorded.
All disbursements are not recorded.	All disbursements are recorded.
Disbursements are recorded for an inappropriate period.	Disbursements are recorded in the period in which they are issued.
Adjustments to inventory prices or quantities are not recorded promptly and not done in the appropriate period.	Adjustments to inventory prices or quantities are recorded promptly and in the appropriate period.
System access to process transactions has not been restricted to the authorized users.	System access to process transactions has been restricted to the authorized users.

1.8.3 Order to Cash (O2C) – Risks and Controls

Order to Cash (OTC or O2C) is a set of business processes that involve receiving and fulfilling customer requests for goods or services. It is a set of business processes that involve receiving and fulfilling customer requests for goods or services. Refer Fig 1.8.1.

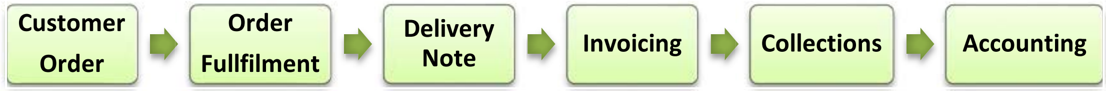


Fig. 1.8.1: Order to Cash Process

Fig. 1.8.1 depicts an O2C cycle that consists of multiple sub-processes including:

1. **Customer Order:** Customer order received is documented;
2. **Order fulfillment:** Order is fulfilled or service is scheduled;
3. **Delivery Note:** Order is shipped to customer or service is performed;

4. **Invoicing:** Invoice is created and sent to customer;
5. **Collections:** Customer sends payment /Collection; and
6. **Accounting:** Payment is recorded in general ledger.

Risks and Control Objectives (Masters-O2C) and Risks and Control Objectives (Transactions-O2C) are provided below in Tables 1.8.3 and 1.8.4 respectively.

Masters

Table 1.8.3: Risks and Control Objectives (Masters-O2C)

Risk	Control Objective
The customer master file is not maintained properly and the information is not accurate.	The customer master file is maintained properly and the information is accurate.
Invalid changes are made to the customer master file.	Only valid changes are made to the customer master file.
All valid changes to the customer master file are not input and processed.	All valid changes to the customer master file are input and processed.
Changes to the customer master file are not accurate.	Changes to the customer master file are accurate.
Changes to the customer master file are not processed in a timely manner.	Changes to the customer master file are processed in a timely manner.
Customer master file data is not up-to-date and relevant.	Customer master file data is up to date and relevant.
System access to maintain customer masters has not been restricted to the authorized users.	System access to maintain customer masters has been restricted to the authorized users.

Transactions

Table 1.8.4: Risks and Control Objectives (Transactions-O2C)

Risk	Control Objective
Orders are processed exceeding customer credit limits without approvals.	Orders are processed only within approved customer credit limits.
Orders are not approved by management as to prices and terms of	Orders are approved by management as to prices and terms of sale.

sale.	
Orders and cancellations of orders are not input accurately.	Orders and cancellations of orders are input accurately.
Order entry data are not transferred completely and accurately to the shipping and invoicing activities.	Order entry data are transferred completely and accurately to the shipping and invoicing activities.
All orders received from customers are not input and processed.	All orders received from customers are input and processed.
Invalid and unauthorized orders are input and processed.	Only valid and authorized orders are input and processed.
Invoices are generated using unauthorized terms and prices.	Invoices are generated using authorized terms and prices.
Invoices are not accurately calculated and recorded.	Invoices are accurately calculated and recorded.
Credit notes and adjustments to accounts receivable are not accurately calculated and recorded.	Credit notes and adjustments to accounts receivable are accurately calculated and recorded.
Goods shipped are not invoiced.	All goods shipped are invoiced.
Credit notes for all goods returned and adjustments to accounts receivable are not issued in accordance with organization policy.	Credit notes for all goods returned and adjustments to accounts receivable are issued in accordance with organization policy.
Invoices are raised for invalid shipments.	Invoices relate to valid shipments.
Credit notes do not pertain to a return of goods or other valid adjustments.	All credit notes relate to a return of goods or other valid adjustments.
Invoices are not recorded in the system.	All invoices issued are recorded.
Credit notes issued are not recorded in the system	All credit notes issued are recorded.
Invoices are recorded in the wrong period.	Invoices are recorded in the appropriate period.
Credit notes are recorded in the wrong period.	Credit notes issued are recorded in the appropriate period.
Cash receipts are not recorded in the period in which they are received.	Cash receipts are recorded in the period in which they are received.

Cash receipts data are not entered correctly.	Cash receipts data are entered for processing accurately.
Cash receipts are not entered in the system for processing.	All cash receipts data are entered for processing.
Cash receipts data are not valid and are not entered in the system for processing more than once.	Cash receipts data are valid and are entered for processing only once.
Cash discounts are not accurately calculated and recorded.	Cash discounts are accurately calculated and recorded.
Collection of accounts receivable is delayed and not properly monitored.	Timely collection of accounts receivable is monitored.
System access to process transactions has not been restricted to the authorized users.	System access to process transactions has been restricted to the authorized users.

1.8.4 Inventory Cycle – Risks and Controls

The **Inventory Cycle** is a process of accurately tracking the on-hand inventory levels for an enterprise. An inventory system should maintain accurate record of all stock movements to calculate the correct balance of inventory. The term "inventory cycle" means different things to companies in different verticals. For those who source, assemble and create inventory, it refers to a time-based process which is basic to understanding how to maximize resources and cash flow. To businesses that buy, store and sell inventory it focuses on the process of understanding, planning and managing inventory levels, from purchasing through more-efficient auditing. The typical phases of the Inventory Cycle for Manufacturers are as follows:

1. **The Ordering phase:** The amount of time it takes to order and receive raw materials.

2. **The Production phase:** The work in progress phase relates to time it takes to convert the raw material to finished goods ready for use by customer.

3. **The finished goods and delivery phase:** The finished goods that remain in stock and the delivery time to the customer. The inventory cycle is measured in number of days.

Risks and Control Objectives (Masters-Inventory) and Risks and Control Objectives (Transactions- Inventory) are provided below in Tables 1.8.5 and 1.8.6 respectively.

Masters

Table 1.8.5: Risks and Control Objectives (Masters-Inventory)

Risk	Control Objective
Invalid changes are made to the inventory management master file.	Only valid changes are made to the inventory management master file.
Invalid changes to the inventory management master file are input and processed.	All valid changes to the inventory management master file are input and processed.
Changes to the inventory management master file are not accurate.	Changes to the inventory management master file are accurate.
Changes to the inventory management master file are not promptly processed.	Changes to the inventory management master file are promptly processed.
Inventory management master file data is not up to date.	Inventory management master file data remain up to date.
System access to maintain inventory masters has not been restricted to the authorized users.	System access to maintain inventory masters has been restricted to the authorized users.

Transactions

Table 1.8.6: Risks and Control Objectives (Transactions-Inventory)

Risk	Control Objective
Adjustments to inventory prices or quantities are not recorded accurately.	Adjustments to inventory prices or quantities are recorded accurately.
Raw materials are received and accepted without valid purchase orders.	Raw materials are received and accepted only if they have valid purchase orders.
Raw materials received are not recorded accurately.	Raw materials received are recorded accurately.
Raw materials received are not recorded in system.	All raw materials received are recorded.
Receipts of raw materials are not recorded promptly and not in the appropriate period.	Receipts of raw materials are recorded promptly and in the appropriate period.
Defective raw materials are not returned promptly to suppliers.	Defective raw materials are returned promptly to suppliers.

Transfers of raw materials to production are not recorded accurately and are not in the appropriate period.	All transfers of raw materials to production are recorded accurately and in the appropriate period.
Direct and indirect expenses associated with production are not recorded accurately and are posted in an inappropriate period.	All direct and indirect expenses associated with production are recorded accurately and in the appropriate period.
Transfers of completed units of production to finished goods inventory are not recorded completely and accurately and are posted in an inappropriate period.	All transfers of completed units of production to finished goods inventory are recorded completely and accurately in the appropriate period.
Finished goods returned by customers are not recorded completely and accurately and are posted in an inappropriate period.	Finished goods returned by customers are recorded completely and accurately in the appropriate period.
Finished goods received from production are not recorded completely and accurately and are posted in an inappropriate period.	Finished goods received from production are recorded completely and accurately in the appropriate period.
Shipments are not recorded in the system.	All shipments are recorded.
Shipments are not recorded accurately.	Shipments are recorded accurately.
Shipments are not recorded promptly and are in an inappropriate period.	Shipments are recorded promptly and in the appropriate period.
Inventory is reduced when goods are not shipped and made based on unapproved customer orders.	Inventory is reduced only when goods are shipped with approved customer orders.
Costs of shipped inventory are not transferred from inventory to cost of sales.	Costs of shipped inventory are transferred from inventory to cost of sales.
Costs of shipped inventory are not accurately recorded.	Costs of shipped inventory are accurately recorded.
Amounts posted to cost of sales does not represent those associated with shipped inventory.	Amounts posted to cost of sales represent those associated with shipped inventory.

Costs of shipped inventory are not transferred from inventory to cost of sales promptly and not done in the appropriate period.	Costs of shipped inventory are transferred from inventory to cost of sales promptly and in the appropriate period.
System access to process inventory related transactions has not been restricted to the authorized users.	System access to process inventory related transactions has been restricted to the authorized users.

1.8.5 Human Resources – Risks and Controls

The **Human Resources (HR)** life cycle refers to human resources management and covers all the stages of an employee's time within a specific enterprise and the role the human resources department plays at each stage. Typical stage of HR cycle includes the following:

1. **Recruiting and On-boarding:** Recruiting is the process of hiring a new employee. The role of the human resources department in this stage is to assist in hiring. This might include placing the job ads, selecting candidates whose resumes look promising, conducting employment interviews and administering assessments such as personality profiles to choose the best applicant for the position. In a small business where the owner performs these duties personally, the HR person would assist in a support role. In some organizations, the recruiting stage is referred to as "hiring support." On-boarding is the process of getting the successful applicant set up in the system as a new employee.

2. **Orientation and Career Planning:** Orientation is the process by which the employee becomes a member of the company's work force through learning her new job duties, establishing relationships with co-workers and supervisors and developing a niche. Career planning is the stage at which the employee and her supervisors work out her long-term career goals with the company. The human resources department may make additional use of personality profile testing at this stage to help the employee determine her best career options with the company.

3. **Career Development:** Career development opportunities are essential to keep an employee engaged with the company over time. After an employee, has established himself at the company and determined his long-term career objectives, the human resources department should try to help him meet his goals, if they're realistic. This can include professional growth and training to prepare the employee for more responsible positions with the company. The

company also assesses the employee's work history and performance at this stage to determine whether he has been a successful hire.

4. **Termination or Transition:** Some employees will leave a company through retirement after a long and successful career. Others will choose to move on to other opportunities or be laid off. Whatever the reason, all employees will eventually leave the company. The role of HR in this process is to manage the transition by ensuring that all policies and procedures are followed, carrying out an exit interview if that is company policy and removing the employee from the system. These stages can be handled internally or with the help of enterprises that provide services to manage the employee life cycle.

Risks and Control Objectives (Configuration-Human Resources) and Risks and Control Objectives (Masters-Human Resources) are provided below in Tables 1.8.7 and 1.8.8 respectively.

Configuration

Table 1.8.7: Risks and Control Objectives (Configuration-Human Resources)

Risk	Control Objective
Employees who have left the company continue to have system access.	System access to be immediately removed when employees leave the company.
Employees have system access in excess of their job requirements.	Employees should be given system access based on a "need to know" basis and to perform their job function.

Masters

Table 1.8.8: Risks and Control Objectives (Masters-Human Resources)

Risk	Control Objective
Additions to the payroll master files do not represent valid employees.	Additions to the payroll master files represent valid employees.
New employees are not added to the payroll master files.	All new employees are added to the payroll master files.
Terminated employees are not removed from the payroll master files.	Terminated employees are removed from the payroll master files.
Employees are terminated without following statutory requirements.	Employees are terminated only within statutory requirements.

Deletions from the payroll master files do not represent valid terminations.	Deletions from the payroll master files represent valid terminations.
Invalid changes are made to the payroll master files.	Only valid changes are made to the payroll master files.
Changes to the payroll master files are not accurate.	Changes to the payroll master files are accurate.
Changes to the payroll master files are not processed in a timely manner.	Changes to the payroll master files are processed in a timely manner.
Payroll master file data is not up to date.	Payroll master file data remain up to date.
Payroll is disbursed to inappropriate employees.	Payroll is disbursed to appropriate employees.
System access to process employee master changes has not been restricted to the authorized users.	System access to process employee master changes has been restricted to the authorized users.

1.8.6 Fixed Assets – Risks and Controls

Fixed Assets process ensures that all the fixed assets of the enterprise are tracked for the purposes of financial accounting, preventive maintenance, and theft deterrence. Fixed assets process ensures that all fixed assets are tracked and fixed asset record maintains details of location, quantity, condition, and maintenance and depreciation status. Typical steps of fixed assets process are as follows:

1. **Procuring an asset:** An asset is most often entered into the accounting system; when the invoice for the asset is entered; into the accounts payable; or purchasing module of the system.

2. **Registering or Adding an asset:** Most of the information needed to set up the asset for depreciation is available at the time the invoice is entered. Information entered at this stage could include; acquisition date, placed-in-service date, description, asset type, cost basis, depreciable basis etc.

3. **Adjusting the Assets:** Adjustments to existing asset information is often needed to be made. Events may occur that can change the depreciable basis of an asset. Further, there may be improvements or repairs made to asset that either adds value to the asset or extend its economic life.

4. **Transferring the Assets:** A fixed asset maybe sold or transferred to another subsidiary, reporting entity, or department within the company. These inter-

company and intra-company transfers may result in changes that impact the asset's depreciable basis, depreciation, or other asset data. This needs to be reflected accurately in the fixed assets management system.

5. **Depreciating the Assets:** The decline in an asset's economic and physical value is called depreciation. Depreciation is an expense which should be periodically accounted on a company's books, and allocated to the accounting periods, to match income and expenses. Sometimes, the revaluation of an asset, may also result in appreciation of its value

6. **Disposing the Assets:** When a fixed asset is no longer in use, becomes obsolete, is beyond repair; the asset is typically disposed. When an asset is taken out of service, depreciation cannot be charged on it. There are multiple types of disposals, such as abandonments, sales, and trade-ins. Any difference between the book value, and realized value, is reported as a gain or loss.

Table 1.8.9 and 1.8.10 given below provide Risks and Control Objectives (Masters-Fixed Assets) and Risks and Control Objectives (Transactions-Fixed Assets) respectively.

Masters

Table 1.8.9: Risks and Control Objectives (Masters-Fixed Assets)

Risk	Control Objective
Invalid changes are made to the fixed asset register and/or master file.	Only valid changes are made to the fixed asset register and/or master file.
Valid changes to the fixed asset register and/or master file are not input and processed.	All valid changes to the fixed asset register and/or master file are input and processed.
Changes to the fixed asset register and/or master file are not accurate.	Changes to the fixed asset register and/or master file are accurate.
Changes to the fixed asset register and/or master file are not promptly processed.	Changes to the fixed asset register and/or master file are promptly processed.
Fixed asset register and/or master file data are not kept up to date.	Fixed asset register and/or master file data remain up to date.
System access to fixed asset master file / system configuration is not restricted to the authorized users.	System access to fixed asset master file / system configuration is restricted to the authorized users.

System configuration pertaining to definition of the depreciation base, depreciation rate, life of asset and accounting of transactions has not been correctly defined.	System configuration pertaining to definition of the depreciation base, depreciation rate, life of asset and accounting of transactions has been correctly defined.

Transactions

Table 1.8.10: Risks and Control Objectives (Transactions-Fixed Assets)

Risk	Control Objective
Fixed asset acquisitions are not accurately recorded.	Fixed asset acquisitions are accurately recorded.
Fixed asset acquisitions are not recorded in the appropriate period.	Fixed asset acquisitions are recorded in the appropriate period.
Fixed asset acquisitions are not recorded.	All fixed asset acquisitions are recorded.
Depreciation charges are not accurately calculated and recorded.	Depreciation charges are accurately calculated and recorded.
Depreciation charges are not recorded in the appropriate period.	All depreciation charges are recorded in the appropriate period.
Fixed asset disposals/transfers are not recorded.	All fixed asset disposals/transfers are recorded.
Fixed asset disposals/transfers are not accurately calculated and recorded.	Fixed asset disposals/transfers are accurately calculated and recorded.
Fixed asset disposals/transfers are not recorded in the appropriate period.	Fixed asset disposals/transfers are recorded in the appropriate period.
Records of fixed asset maintenance activity are not accurately maintained.	Records of fixed asset maintenance activity are accurately maintained.
Fixed asset maintenance activity records are not updated in a timely manner.	Fixed asset maintenance activity records are updated in a timely manner.
Accounting entries pertaining to acquisition, disposals, transfers, retirement are not recorded in the correct GL account.	Accounting entries pertaining to acquisition, disposals, transfers, retirement are recorded in the correct GL account.

System access to process fixed asset transactions has not been restricted to the authorized users.	System access to process fixed asset transactions has been restricted to the authorized users.

1.8.7 General Ledger – Risks and Controls

General Ledger (GL) process refers to the process of recording the transactions in the system to finally generating the reports from financial transactions entered in the system. The input for GL Process Flow is the financial transactions and the outputs are various types of financial reports such as balance sheet, profit and loss a/c, funds flow statement, ratio analysis, etc.

The typical steps in general ledger process flow are as follows:

1. Entering financial transactions into the system
2. Reviewing Transactions
3. Approving Transactions
4. Posting of Transactions
5. Generating Financial Reports

Risks and Control Objectives (Configuration- General Ledger); Risks and Control Objectives (Masters-General Ledge) and Risks and Control Objectives (Transactions-General Ledger) are provided below in Tables 1.8.11, 1.8.12 and 1.8.13 respectively.

Configuration

Table 1.8.11: Risks and Control Objectives (Configuration-General Ledger)

Risk	Control Objective
Unauthorized general ledger entries could be passed.	Access to general ledger entries is appropriate and authorized.
System functionality does not exist to segregate the posting and approval functions.	System functionality exists to segregate the posting and approval functions.
Interrelated balance sheets and income statement accounts do not undergo automated reconciliations to confirm accuracy of such accounts.	Interrelated balance sheets and income statement accounts undergo automated reconciliations to confirm accuracy of such accounts.
Systems do not generate reports of all	Systems generate reports of all recurring

recurring and non-recurring journal entries for review by management for accuracy.	and nonrecurring journal entries for review by management for accuracy.
Non-standard journal entries are not tracked and are inappropriate.	All non-standard journal entries are tracked and are appropriate.
Out-of-balance entries are not prohibited.	Out-of-balance entries are prohibited.
Enterprise wide consolidation, including standard inter-company eliminations, is not automated and not performed.	Enterprise wide consolidation, including standard inter-company eliminations, is automated and performed.
Variance reports are not generated for use to identify posting errors/out-of-balance conditions.	Variance reports are generated for use to identify posting errors/out-of-balance conditions.
System controls are not in place for appropriate approval of write-offs.	System controls are in place for appropriate approval of write-offs.
Journal entries of exceptional amount that were posted to the general ledger during the month are not flagged by the system and not subsequently reviewed for accuracy and approved by the controller or CFO after month-end.	Journal entries of exceptional amount that were posted to the general ledger during the month are flagged by the system and subsequently reviewed for accuracy and approved by the controller or CFO after month-end.
Automated amortization timing, periods and methods are not appropriate and not accurately entered.	Automated amortization timing, periods and methods are appropriate and accurately entered.
Standard, recurring period-end journal entries submitted from subsidiary ledger systems are not automated, not appropriately approved and not entered accurately.	Standard, recurring period-end journal entries submitted from subsidiary ledger systems are automated, appropriately approved and entered accurately.
Transactions can be recorded outside of financial close cut-off requirements.	Transactions cannot be recorded outside of financial close cut-off requirements.
The sources of all entries are not readily identifiable.	The sources of all entries are readily identifiable.
Transactions are not rejected, accepted and identified, on exception reports in the event of data exceptions.	Transactions are rejected, or accepted and identified, on exception reports in the event of data exceptions.

Account mappings are not up to date.	Account mappings are up to date.
Adding to or deleting general ledger accounts are not limited to authorized accounting department personnel.	Adding to or deleting general ledger accounts is limited to authorized accounting department personnel.

Masters

Table 1.8.12: Risks and Control Objectives (Masters-General Ledger)

Risk	Control Objective
General ledger master file change reports are not generated by the system and are not reviewed as necessary by an individual who does not input the changes.	General ledger master file change reports are generated by the system and reviewed as necessary by an individual who does not input the changes.
A standard chart of accounts has not been approved by management and is not utilized within all entities of the corporation.	A standard chart of accounts has been approved by management and is not utilized within all entities of the corporation.

Transactions

Table 1.8.13: Risks and Control Objectives (Transactions-General Ledger)

Risk	Control Objective
General ledger balances are not reconciled to sub ledger balances and such reconciliation are not reviewed for accuracy and not approved by supervisory personnel.	General ledger balances reconcile to sub ledger balances and such reconciliation are reviewed for accuracy and approved by supervisory personnel.
Interrelated balance sheets and income statement accounts do not undergo automated reconciliation to confirm accuracy of such accounts.	Interrelated balance sheets and income statement accounts undergo automated reconciliation to confirm accuracy of such accounts.
Account codes and transaction amounts are not accurate and not complete, and exceptions are not reported.	Account codes and transaction amounts are accurate and complete, with exceptions reported.

A report of all journal entries completed as part of the closing process is not reviewed by management to confirm the completeness and appropriateness of all recorded entries.	A report of all journal entries completed as part of the closing process is reviewed by management to confirm the completeness and appropriateness of all recorded entries.
Actual-to-actual, actual-to-budget and yield reports are not produced from the general ledger system monthly prior to the final close of the general ledger. Reports are not distributed to and reviewed by the controller and CFO. Unusual amounts or variances are not investigated and reclassified when applicable.	Actual-to-actual, actual-to-budget and yield reports are produced from the general ledger system monthly prior to the final close of the general ledger. Reports are distributed to and reviewed by the controller and CFO. Unusual amounts or variances are investigated and re-classified when applicable.
Entries booked in the close process are not complete and accurate.	Entries booked in the close process are complete and accurate.

1.9 REGULATORY AND COMPLIANCE REQUIREMENTS

Major corporations worldwide have used Information Technology (IT) to stay ahead in business. The competitive edge in terms of fast information flow, to support the business, can be an important factor between success and failure.

The efficiency of an enterprise depends on the quick flow of information across the complete supply chain i.e., from the customer to manufacturers to the suppliers. With the globalization of the market place coupled with competition and increasing customer expectations enterprises should address certain fundamental areas like lowering costs in the supply chain, reducing throughput times, optimizing stock levels, improving product quality, improving service to the customer, efficiently handling cross border data flow etc. Today’s IT systems achieve all this.

The core to any enterprise’s success is to have an efficient and effective financial information system to support decision-making and monitoring. The risks, controls and security of such systems should be clearly understood to pass an objective opinion about the adequacy of control in an IT environment.

1.9.1 The Companies Act, 2013

The Companies Act, 2013 has two very important Sections - **Section 134** and **Section 143**, which have a direct impact on the audit and accounting profession.

(i) Section 134

Section 134 of the Companies Act, 2013 on "Financial statement, Board's report, etc." states inter alia:

The **Directors' Responsibility Statement** referred to in clause (c) of sub-section (3) shall state that:

- the Directors had taken proper and sufficient care for the maintenance of adequate accounting records in accordance with the provisions of this Act for safeguarding the assets of the company and for preventing and detecting fraud and other irregularities;
- the Directors, in the case of a listed company, had laid down internal financial controls to be followed by the company and that such internal financial controls are adequate and were operating effectively.

Explanation: For the purposes of this clause, the term "Internal Financial Controls" means the policies and procedures adopted by the company for ensuring the orderly and efficient conduct of its business, including adherence to company's policies, the safeguarding of its assets, the prevention and detection of frauds and errors, the accuracy and completeness of the accounting records, and the timely preparation of reliable financial information the directors had devised proper systems to ensure compliance with the provisions of all applicable laws and that such systems were adequate and operating effectively.

(ii) Section 143

Section 143, of the Companies Act 2013, on "Powers and duties of auditors and auditing standards" states inter alia:

Section 143(3) contains the **Auditor's Report** which states:

"whether the company has adequate internal financial controls system in place and the operating effectiveness of such controls";

When we talk in terms of "adequacy and effectiveness of controls"; it refers to the adequacy of the control design and whether the control has been working effectively during the relevant financial year.

For example, let us assume that a company has a sales invoicing control wherein all sales invoices raised by the salesman which is greater than` 50,000/- are reviewed and approved by the sales manager. In terms of the of the control design this control may seem adequate. However, if during audit, it was found that, during the year, there were many invoices raised by the salesman which was greater than ` 50,000/- and not reviewed and approved by the sales manager. In such a case, although the control design was adequate, the control was not working effectively, due to many exceptions without proper approval.

As per ICAI's "Guidance Note on Audit of Internal Financial Controls Over Financial Reporting":

Clause (i) of Sub-section 3 of Section 143 of the Companies Act, 2013 ("The 2013 Act" or "The Act") requires the auditors' report to state whether the company has adequate internal financial controls system in place and the operating effectiveness of such controls.

I. Management's Responsibility

The 2013 Act has significantly expanded the scope of internal controls to be considered by the management of companies to cover all aspects of the operations of the company. Clause (e) of Sub-section 5 of Section 134 to the Act requires the directors' responsibility statement to state that the directors, in the case of a listed company, had laid down internal financial controls to be followed by the company and that such internal financial controls are adequate and were operating effectively.

Clause (e) of Sub-section 5 of Section 134 explains the meaning of the term, "internal financial controls" as "the policies and procedures adopted by the company for ensuring the orderly and efficient conduct of its business, including adherence to company's policies, the safeguarding of its assets, the prevention and detection of frauds and errors, the accuracy and completeness of the accounting records, and the timely preparation of reliable financial information."

Rule 8(5)(viii) of the Companies (Accounts) Rules, 2014 requires the Board of Directors' report of all companies to state the details in respect of adequacy of internal financial controls with reference to the financial statements.

The inclusion of the matters relating to internal financial controls in the directors' responsibility statement is in addition to the requirement for the directors to state that they have taken proper and sufficient care for the maintenance of adequate accounting records in accordance with the provisions of the 2013 Act, for safeguarding the assets of the company and for preventing and detecting fraud and other irregularities.

II. Auditors' Responsibility

The auditor's objective in an audit of internal financial controls over financial reporting is to express an opinion on the effectiveness of the company's internal financial controls over financial reporting and the procedures in respect thereof are carried out along with an audit of the financial statements. Because a company's internal controls cannot be considered effective if one or more material weakness exists, to form a basis for expressing an opinion, the auditor should plan and perform the audit to obtain sufficient appropriate evidence to obtain reasonable assurance about whether material weakness exists as of the date specified in management's assessment. A material weakness in internal financial controls may exist even when the financial statements are not materially misstated.

III. Corporate Governance Requirements

Corporate Governance is the framework of rules and practices by which a board of directors ensures accountability, fairness, and transparency in a company's relationship with its all stakeholders (financiers, customers, management, employees, government, and the community).

The Corporate Governance framework consists of:

(i) explicit and implicit contracts between the company and the stakeholders for distribution of responsibilities, rights, and rewards.

(ii) procedures for reconciling the sometimes-conflicting interests of stakeholders in accordance with their duties, privileges, and roles, and

(iii) procedures for proper supervision, control, and information-flows to serve as a system of checks-and-balances.

1.9.2 Information Technology Act (IT Act)

This Act aims to provide the legal infrastructure for e-commerce in India. And the cyber laws have a major impact for e-businesses and the new economy in India. So, it is important to understand what are the various perspectives of the IT Act, 2000 (as amended in 2008) and what it offers.

The Act also aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability.

I. Computer Related Offences

Let us look at some common cyber-crime scenarios which can attract prosecution as per the penalties and offences prescribed in IT Act 2000 (amended via 2008) Act.

- **Harassment via fake public profile on social networking site:** A fake profile of a person is created on a social networking site with the correct address, residential information or contact details but he/she is labelled as 'prostitute' or a person of 'loose character'. This leads to harassment of the victim.
- **Email Account Hacking:** If victim's email account is hacked and obscene emails are sent to people in victim's address book.
- **Credit Card Fraud:** Unsuspecting victims would use infected computers to make online transactions.
- **Web Defacement:** The homepage of a website is replaced with a pornographic or defamatory page. Government sites generally face the wrath of hackers on symbolic days.
- **Introducing Viruses, Worms, Backdoors, Rootkits, Trojans, Bugs:** All these are some sort of malicious programs which are used to destroy or gain access to some electronic information.
- **Cyber Terrorism:** Many terrorists use virtual (Drive, FTP sites) and physical storage media (USB's, hard drives) for hiding information and records of their illicit business.
- **Online sale of illegal Articles:** Where sale of narcotics, drugs weapons and wildlife is facilitated by the Internet.
- **Cyber Pornography:** Among the largest businesses on Internet, pornography may not be illegal in many countries, but child pornography is.
- **Phishing and Email Scams:** Phishing involves fraudulently acquiring sensitive information through masquerading oneself as a trusted entity (e.g. usernames, Passwords, credit card information).
- **Theft of Confidential Information:** Many business organizations store their confidential information in computer systems. This information is targeted by rivals, criminals and disgruntled employees.
- **Source Code Theft:** A Source code generally is the most coveted and important "crown jewel" asset of a company.

- **Cyber Crime:** The term 'Cyber Crime' finds no mention either in The Information Technology Act 2000 or in any legislation of the Country. Cyber Crime is not different than the traditional crime. The only difference is that in Cyber Crime the computer technology is involved and thus it's a Computer related crime. This can be explained by the following instance:
  - **Traditional Theft:** 'A' thief enters in B's house and steals an object kept in the house.
  - **Hacking:** Many business organizations store their confidential information in computer systems which is often targeted by rivals, criminals and disgruntled employees. Hacking generally refers to unauthorized intrusion into a computer or a network. This may be done by either altering system or security features to accomplish a goal that differs from the original purpose of the system. For example - Mr. A, a cyber-criminal while sitting in his own house, through his computer hacks the computer of Mr. B and steals the data saved in B's computer without physically touching the computer or entering in B's house.

II. Advantages of Cyber Laws

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber-crimes. We need such laws so that people can perform purchase transactions over the Net without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.

In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format. The Act has also proposed a legal framework for the authentication and origin of electronic records/communications through digital signature.

From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects which are as follows:

- The implications for the e-businesses would be that email would now be a valid and legal form of communication in India that can be duly produced and approved in a court of law.
- Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.
- Digital signatures have been given legal validity and sanction in the Act.

- The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates.
- The Act now allows Government to issue notification on the web thus heralding e-governance.
- The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.
- The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions.
- The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date.

Under the IT Act, 2000, it shall now be possible for corporates to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding ₹ 1 crore.

III. Privacy

The main principles on data protection and privacy enumerated under the IT Act, 2000 are:

- defining 'data', 'computer database', 'information', 'electronic form', 'originator', 'addressee' etc.
- creating civil liability if any person accesses or secures access to computer, computer system or computer network
- creating criminal liability if any person accesses or secures access to computer, computer system or computer network
- declaring any computer, computer system or computer network as a protected system
- imposing penalty for breach of confidentiality and privacy
- setting up of hierarchy of regulatory authorities, namely adjudicating officers, the Cyber Regulations Appellate Tribunal etc.

Example - Privacy Policy

A sample privacy policy is given below which highlights key aspects of how and what type of information is collected from the customer, how it is used and secured and options for user providing the information:

“At ABC Ltd., we take your privacy very seriously. Because of this, we want to provide you with explicit information on how we collect, gather, and identify information during your visit to our site. This information may be expanded or updated as we change or develop our site. For this reason, we recommend that you review this policy from time-to-time to see if anything has changed. Your continued use of our site signifies your acceptance of our privacy policy.”

Personally, identifiable information refers to information that tells us specifically who you are, such as your name, phone number, email or postal address. In many cases, we need this information to provide the personalized or enhanced service that you have requested. The amount of personally identifiable information that you choose to disclose to ABC Ltd. is completely up to you. The only way we know something about you personally is if you provide it to us in conjunction with one of our services.

What information do we collect and how do we use it?

- ABC Ltd. Collects information on our users by your voluntary submissions (e.g., when you sign up for a white paper or request product information). We also collect, store and accumulate certain non-personally identifiable information concerning your use of this web site, such as which of our pages are most visited.
- The information ABC Ltd. collects is used in a variety of ways: for internal review; to improve the content of the site, thus making your user experience more valuable; and to let you know about products and services of interest.

Email

- If you have provided us your email address, ABC Ltd. Periodically sends promotional emails about products offered by us. If you do not wish to receive email information from ABC Ltd. please let us know by emailing us.
- ABC Ltd. does not sell, rent, or give away your personal information to third parties. By using our web site, you provide consent to the collection and use of the information described in this by Privacy Policy of ABC Ltd.”

IV. Sensitive Personal Data Information(SPDI)

Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules 2011 formed under Section 43A of the Information Technology Act 2000 define a data protection framework for the processing of digital data by Body Corporate.

Scope of Rules: Currently the Rules apply to Body Corporate and digital data. As per the IT Act, Body Corporate is defined as "Any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities."

The present scope of the Rules excludes from its purview several actors that do or could have access to Big Data or use Big Data practices. The Rules would not apply to government bodies or individuals collecting and using Big Data. Yet, with technologies such as IoT (Internet of Things) and the rise of Smart Cities across India – a range of government, public, and private organizations and actors could have access to Big Data.

Definition of Personal and Sensitive Personal data: Rule 2(i) defines personal information as "information that relates to a natural person which either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person."

Rule 3 defines sensitive personal information as Passwords; Financial information; Physical/physiological/mental health condition; Sexual orientation; Medical records and history; and Biometric information.

The present definition of personal data hinges on the factor of identification (data that is capable of identifying a person). Yet this definition does not encompass information that is associated to an already identified individual - such as habits, location, or activity.

The definition of personal data also addresses only the identification of 'such person' and does not address data that is related to a particular person but that also reveals identifying information about another person - either directly - or when combined with other data points. By listing specific categories of sensitive personal information, the Rules do not account for additional types of sensitive personal information that might be generated or correlated through the use of Big Data analytics.

Importantly, the definitions of sensitive personal information or personal information do not address how personal or sensitive personal information - when anonymized or aggregated – should be treated.

Consent to collect: Rule 5(1) requires that Body Corporate should, prior to collection, obtain consent in writing through letter or fax or email from the provider of sensitive personal data regarding the use of that data.

In a context where services are delivered with little or no human interaction, data is collected through sensors, data is collected on a real time and regular basis, and data is used and re-used for multiple and differing purposes - it is not practical, and often not possible, for consent to be obtained through writing, letter, fax, or email for each instance of data collection and for each use.

Consent to Disclosure: Rule 6 provides that Disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation:

SUMMARY

Technology is the enabler of business process automation (BPA), and it can automate business processes to the point where human intervention is unnecessary. Automation can save time and money, delight customers who no longer must wait in line for a person to assist them with a transaction, and avoid human errors.

But not every business process is a good fit for automation, so it's incumbent upon companies to determine which processes are best suited to automation and which ones are best handled manually. How do companies select which business processes to automate? Companies start by looking at the strategic and operating drivers for process improvement in their organizations and industries. For instance, in today's global market, nearly every company is feeling pressure to get goods to market quickly and to be first to market whenever possible. In a highly price-competitive environment, companies are also under great pressure to economize their operations to improve their profitability. Consequently, companies look to automate business processes that are time and resource intensive operationally, that are subject to human error, and that can be accelerated with automated process improvements achievable through computers and technology. If automating business processes speeds product to market, improves revenue, reduces operating expenses so margins can improve and brings efficiency and effectiveness in the enterprise, the case for automation is substantiated.

Enhanced automated controls within accounting and transaction recording applications can control risk much before they can actually materialize. In addition, companies are under added pressure as regulators, rating agencies and stock exchanges drive improved standards of risk management at an enterprise level, with special emphasis on good corporate governance. Enterprises are therefore in the process of adopting a variety of automated controls to help them combat risk and advance to a proactive approach that reduces the incidence of errors or focuses on them well before the point of impact.

By definition, an automated control is a mechanism or device inside an application, interface or appliance that enforces or controls a rule-set or validation on one or more conditions inside a process. A very simple example of an automated control in accounting parlance is a "drop-down list" of vendors to ensure that the user selects one of the multiple choices provided therein. This would ensure that the transaction is conducted with the authorized set of vendors, which have been set elsewhere by another team that is responsible for vendor on-boarding. Similarly, there are several applications of automated controls in accounting with the prime objective of:

- Mitigating/Eliminating Frauds through enforced segregation of duties and ensuring adherence to a set of delegation of financial powers
- Business Process Improvement through elimination of manual controls thereby enhancing efficiency and reducing costs
- Reduced Audit Costs by shifting from "transaction" audit to "controls" audit
- Adherence to Regulatory Compliance requirements such as Companies Act 2013, IT Act, and the likes, entailing testing of key controls through sampling techniques, which again can be reduced substantially by monitoring the effectiveness of automated controls.

IT is primary driver for enterprises to survive and thrive in this digital age. Regulators have recognized critical importance of IT and hence facilitate digital economy by providing legislative framework and mandating compliances as required. The IT Act, 2000 and Companies have been updated to meet the needs of digital economy. Protection of privacy and personal information is also mandated. Cyber-crime is a reality of digital world when operates without geographical boundaries. Various types of computer related defines have been defined and penalties specified for these offences. Digitization of business processes is a should for modern enterprises and this leads to new risks which should be mitigated by implementing appropriate controls.

TEST...YOUR KNOWLEDGE

Theoretical Questions

1. In an enterprise, explain the difference between various business processes - Operational Processes, Supporting Processes and Management Processes through an example.

   (Refer Section 1.2.1)

2. What are the benefits of Automating Business Processes?

   (Refer Section 1.3.2)

3. As an entrepreneur, your business may face all kinds of risks related from serious loss of profits to even bankruptcy. What could be the possible Business Risks?

   (Refer Section 1.4.4)

4. ERM provides a framework for risk management, which typically involves identifying events or circumstances relevant to the organization's objectives. Discuss the main components of Enterprise Risk Management Framework.

   (Refer Section 1.6.2)

5. Explain the five components of Internal Control, as per SA315.

   (Refer Section 1.5.4)

6. As a student, you are supposed to present a PowerPoint presentation on the topic "Advantages and Limitations of Flowcharts" during your practical test. What shall be the relevant content?

   (Refer Section 1.7.1)

7. Give two examples each of the Risks and Control Objectives for the following business processes:

   a. Procure to Pay (Refer Section 1.8.2)

   b. Order to Cash (Refer Section 1.8.3)

   c. Inventory Cycle (Refer Section 1.8.4)

8. Explain the salient features of Section 134 & Section 143 of the Companies Act 2013.

   (Refer Section 1.9.1)

9. Give five examples of computer related offences that can be prosecuted

under the IT Act 2000 (amended via 2008).

(Refer Section 1.9.2)

10. Draw a Flowchart for the following process:

Leebay is a new e-commerce web site that is setting up business in India. Leebay and their partner bank Paxis have come up with a joint promotion plan for which the following offers are proposed. Customers can either log in through a mobile app or directly from the website:

(1) If the payment mode chosen is 'Paxis Credit', then a 20% discount is given to the user.

(2) If the payment mode chosen is 'Paxis Debit', then a 10% discount is given to the user.

(3) If other payment modes are used, then no discount is given.

Also, to promote the downloads of its new smart phone app, the company has decided to give the following offer:

(1) If the purchase mode is 'Mobile App', then no surcharge is levied on the user.

(2) If any other purchase mode is used, then additional 5% surcharge is levied on the user. This surcharge is applied on the bill after all necessary discounts have been applied.

With bill amount, payment mode and purchase mode as inputs, draw a flowchart for the billing procedure for Leebay.

Solution: The variables used are defined as follows:

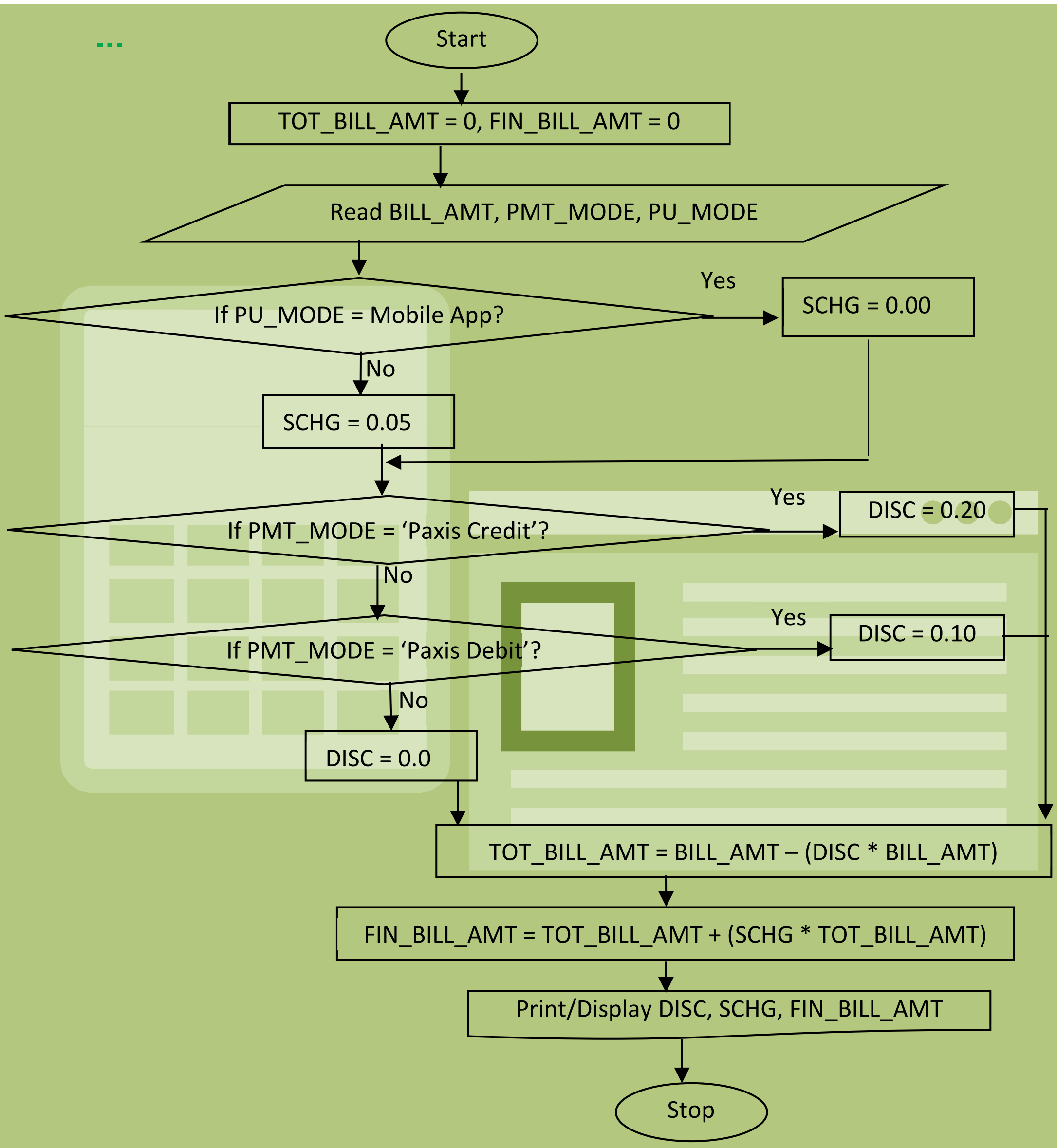
PU_MODE: Purchase Mode BILL_AMT: Initial Bill Amount

TOT_BILL_AMT: Bill Amount after Discount SCHG: Surcharge

FIN_BILL_AMT: Final Bill Amount after Surcharge DISC: Discount

PMT_MODE: Payment Mode

…


Start
TOT_BILL_AMT = 0, FIN_BILL_AMT = 0
Read BILL_AMT, PMT_MODE, PU_MODE
If PU_MODE = Mobile App?
Yes
SCHG = 0.00
No
SCHG = 0.05
If PMT_MODE = 'Paxis Credit'?
Yes
DISC = 0.20
No
If PMT_MODE = 'Paxis Debit'?
Yes
DISC = 0.10
No
DISC = 0.0
TOT_BILL_AMT = BILL_AMT – (DISC * BILL_AMT)
FIN_BILL_AMT = TOT_BILL_AMT + (SCHG * TOT_BILL_AMT)
Print/Display DISC, SCHG, FIN_BILL_AMT
Stop

Multiple Choice Questions

1. Which of the following is not an objective of Enterprise Information Systems?

   (a) Reduce service cycles

   (b) Identify manual processes

   (c) Reduce costs

   (d) Increase operational efficiency

2. Which one of the following represents Operational Processes?

   (a) Deals with legal compliance

   (b) Deal with the core business and value chain

   (c) Deal with core processes and functions within an organization

   (d) Deals with measuring, monitoring and control activities

3. Which one of the following is not a benefit of Business Process Automation?

   (a) Reduce turnaround time

   (b) Operational efficiency

   (c) Legal compliance

   (d) Reduce costs

4. Which of the following is not a Business Risk?

   (a) Strategic

   (b) Financial

   (c) Operational

   (d) Environmental

5. Which one of the following does not represent a system of Internal Control?

   (a) Meeting sales targets

   (b) Safeguarding assets

   (c) Prevention and detection of fraud and error

   (d) Completeness of accounting records

6. Which of the following is not a Flowcharting symbol?

   (a) Process

   (b) Decision

   (c) Document

   (d) Risk

7. Which of the following is not a component of Enterprise Risk Management Framework?

   (a) Internal environment

   (b) Organization chart

(c) Objective setting

(d) Event identification

8. Which one of the following is not an objective of Internal Control?

(a) Compliance with applicable laws and regulations

(b) Meeting sales targets

(c) Reliability of reporting

(d) Effectiveness and efficiency of operations

9. Which one of the following deals with Section 143 of the Companies Act 2013?

(a) Acquisition and Mergers

(b) Powers and duties of Board of Directors

(c) Powers and duties of auditors and auditing standards

(d) Penalties due to non-compliance

10. Which one of the following is not defined as Sensitive Personal Information?

(a) Home address

(b) Password

(c) Financial information

(d) Biometric information

11. Which of the following does not form part of Human Resource (HR) Management?

(a) Training and Development

(b) Career Development

(c) Leadership Management

(d) Invoicing

12. Which of the following is not a benefit of documentation of Business Process Automation implementation?

(a) Clarity on the process

(b) To find the bottlenecks

(c) Identify the source of inefficiency

(d) Design new policy format

13. A store supplies goods only on receipt of advance payment. Once payment is received, an intimation to customer is sent for receipt of payment. This is a good example of ________?

    (a) Supply Chain Management

    (b) Customer Relationship Management

    (c) Order to Cash Cycle

    (d) Enterprise Information System

14. A huge oil spill from an oil well run by British Petroleum, one of largest oil companies in world, resulted in an assessed environmental damage of about USD 20 Billion. The company expanded an amount of USD 2 Billion on promotional ads informing the world that it is an environmentally friendly company. The promotional ads were done to prevent company from which damage?

    (a) Strategic

    (b) Operational

    (c) Financial

    (d) Reputational

15. A bank shares financial data of borrower with third-party without consent of borrower. The bank has violated _______ of Sensitive Information and Personal Data Rules, 2011.

    (a) Rule 3

    (b) Rule 4

    (c) Rule 5

    (d) Rule 6

Answers

1.	(b)	**2.**	(b)	**3.**	(c)	**4.**	(d)	**5.**	(a)	**6.**	(d)	**7.**	(b)
8.	(b)	**9.**	(c)	**10.**	(a)	**11.**	(d)	**12.**	(d)	**13.**	(b)	**14.**	(d)
15.	(d)												

CHAPTER 2

FINANCIAL AND ACCOUNTING SYSTEMS

LEARNING OUTCOMES

After reading this chapter, you will be able to -

Understand about working of Financial and Accounting System.

❑ Grasp the knowledge about Integrated and Non-Integrated Systems.

❑ Comprehend about business process modules.

❑ Acknowledge about Reporting Systems, Data Analytics, Business Intelligence and Fundamentals of XBRL.

❑ Comprehend about regulatory and compliance requirements and their correlation with financial and accounting systems.

CHAPTER OVERVIEW

- Integrated & Non Integrated System
- Business Process Modules and Their Integration with Financial & Accounting Systems
- Reporting Systems and Management Information Systems
- Data Analytics and Business Intelligence
- Business Reporting and Fundamentals of XBRL
- Applicable Regulatory & Compliance Requirements

2.1 INTRODUCTION

This chapter is meant for providing an insight to Financial and Accounting Systems, its working, audit and its use for business management and development. Financial and Accounting Systems forms an integral part of any business and acts as a backbone for it. Financial and Accounting systems may include other aspects of business management like human resource, inventory, Customer Relationship Management (CRM), etc. After going through this chapter, a student is expected to understand about–

- What is a system?
- What is ERP System?
- What is a Financial and Accounting system?
- How to use it for different purposes like accounting, auditing, business management, etc.?
- How to assess risks and controls of any Financial and Accounting System?

In the process of learning about Financial and Accounting systems, there can be different angles to view the same thing and to understand it in a better way, we shall be viewing Financial and Accounting Systems from many different angles. At time of understanding the system from one angle, another angle must be kept in mind and cannot be ignored. Chartered Accountants are supposed to be experts in accounting as well as accounting systems. Financial and Accounting Systems does not necessarily mean Software or Computerized Systems only. It may include many other aspects also.

Fig. 2.1.1 depicts different perspectives of the same view through different Professionals.

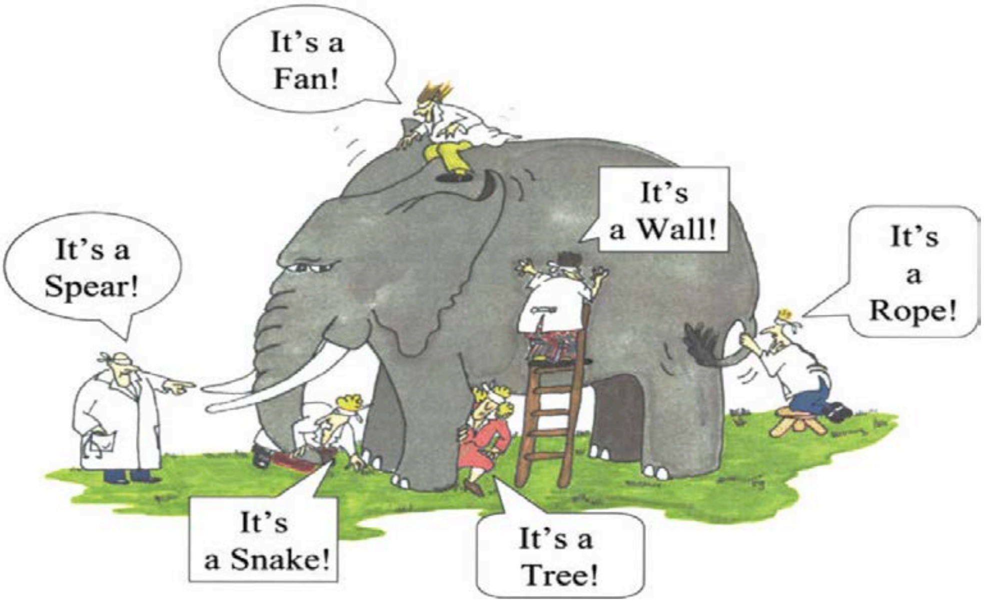


Fig. 2.1.1: Different perspectives from different Professionals

Different Requirements from Different Persons

- **Accountants View** – Balance Sheet and Profit & Loss Account must be prepared easily without putting much time / efforts.
- **Auditors View** – Balance Sheet and Profit & Loss Account must be correct at any point of time.
- **Business Manager / Owner's View** – I need right information at right point of time for right decision making.

It is the job of any Financial and Accounting System to cater to needs of all the users simultaneously. Hence, we shall discuss Financial and Accounting Systems from all the possible angles.

2.2 ERP AND NON-INTEGRATED SYSTEMS

2.2.1 What is a System?

What is a system and how this word relates to Financial and Accounting aspect? This is important for us to understand. Many a times this word is mistakenly understood as something relating to computer / software / information technology etc. Here it is suggested to make this point very clear that a system may or may not be related with computer / software / information technology etc. Software / Computer / Hardware may or may not form part of overall system.

Dictionary meaning of the word System is -

"A set of principles or procedures per which something is done; an organized scheme or method"

or

"A set of things working together as parts of a mechanism or an interconnecting network; a complex whole"

The word "system" can be explained in a simple way as, "a set of detailed methods, procedures and routines created to carry out a specific activity, perform a duty, or solve a problem". It is an organized, purposeful structure that consists of interrelated and interdependent elements (components, entities, factors, members, parts etc.).

These elements continually influence one another (directly or indirectly) to maintain their activity and the existence of the system, to achieve the goal of the system.

All systems generally have -

(a) Inputs, outputs and feedback mechanisms,

(b) Maintain an internal steady-state despite a changing external environment,

(c) Have boundaries that are usually defined by the system observer.

Systems may consist of sub-system also which are a part of a larger system. Systems stop functioning when an element is removed or changed significantly. Together, they allow understanding and interpretation.

Human body is natural and a complete system. We know about the word "Eco System". Every human body is a part of Eco System. An ecosystem includes all the living things (plants, animals and organisms) in each area, interacting with each other, and with their non-living environments (weather, earth, sun, soil, climate, and atmosphere). In an ecosystem, each organism has its' own niche or role to play.

In this chapter, we are discussing system for business finance and accounting.

A system includes defined methods and process to perform an activity. So basically, processes are important components in any system.

2.2.2 What is a Process?

In the systems engineering arena, a **Process** is defined as a sequence of events that uses inputs to produce outputs. This is a broad definition and can include sequences as mechanical as reading a file and transforming the file to a desired output format; to taking a customer order, filling that order, and issuing the customer invoice.

From a business perspective, a Process is a coordinated and standardized flow of activities performed by people or machines, which can traverse functional or departmental boundaries to achieve a business objective and creates value for internal or external customers.

2.2.3 Concepts in Computerized Accounting Systems

As we are discussing about Financial & Accounting Systems, it is necessary to discuss some concepts to understand Financial and Accounting systems in a better way.

I. Types of Data

Every accounting systems stores data in two ways: **Master Data** and **Non-Master Data** (or Transaction Data) as shown in the Fig. 2.2.1.

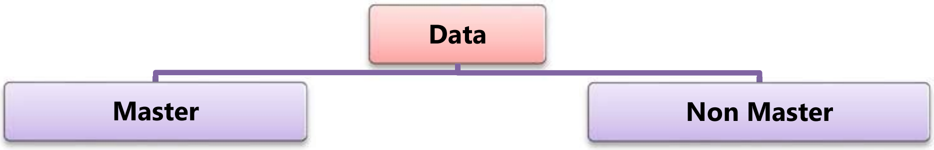


Fig. 2.2.1: Types of Data

- ♦ **Master Data:** Relatively permanent data not expected to change frequently.
- ♦ **Non-Master Data:** Non-permanent data and expected to change frequently.

A. **Master Data:** As defined above, master data is relatively permanent data that is not expected to change again and again. It may change, but not again and again. In accounting systems, there may be following type of master data as shown in the Fig. 2.2.2.

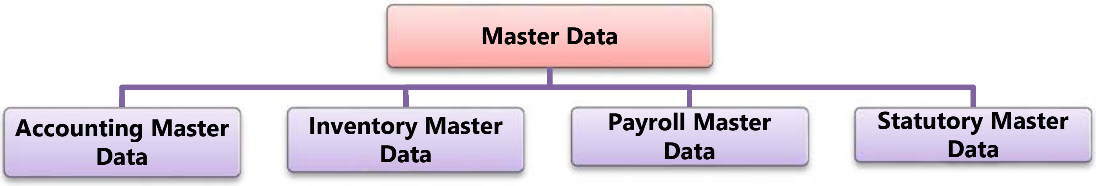


Fig. 2.2.2: Types of Master Data in Financial and Accounting Systems

a. **Accounting Master Data –** This includes names of ledgers, groups, cost centres, accounting voucher types, etc. E.g. Capital Ledger is created once and not expected to change frequently. Similarly, all other ledgers like, sales, purchase, expenses and income ledgers are created once and not expected to change again and again. Opening balance carried forward from previous year to next year is also a part of master data and not expected to change.

b. **Inventory Master Data –** This includes stock items, stock groups, godowns, inventory voucher types, etc. Stock item is something which bought and sold for business purpose, trading goods. E.g. If a person is into the business of dealing in white goods, stock items shall be Television, Fridge, Air Conditioner, etc. For a person running a medicine shop, all types of medicines shall be stock items for him/her.

c. **Payroll Master Data –** Payroll is another area connecting with Accounting Systems. Payroll is a system for calculation of salary and recoding of transactions relating to employees. Master data in case of payroll can be names of employees, group of employees, salary structure, pay heads, etc. These data are not expected to change frequently. E.g. Employee created in the system will remain as it is for a longer period of time, his/her salary structure may change but not frequently, pay heads associated with his/her salary structure will be relatively permanent.

d. **Statutory Master Data –** This is a master data relating to statute/law. It may be different for different type of taxes. E.g. Goods and Service Tax (GST), Nature of Payments for Tax Deducted at Source (TDS), etc. This data also shall be relatively permanent. We don’t have any control on this data as statutory changes are made by Government and not by us. In case of change in tax rates, forms, categories, we need to update/change our master data.

All business process modules must use common master data.

B. **Non-Master Data:** It is a data which is expected to change frequently, again and again and not a permanent data. E.g. Amounts recorded in each transaction shall be different every time and expected to change again and again. Date recorded in each transaction is expected to change again and again and will not be constant in all the transactions.

To understand the concept of master data and non-master data in a simple way, let us co-relate this with ourselves using following example.

Our Personal Master Data –Our Name, Name of Parents, Address, Blood Group, Gender, Date of Birth, etc. is a personal master data and not expected to change. Our address may change, but not frequently. Contrary to this, there may be some information about us which may fall in the category of non- master data, i.e. not a permanent data. E.g. Date of Birth is master data but age is a non- master data, weight is a non-master data, our likes, dislikes again is a non-master data.

C. **Why Master and Non-Master Data?**

Basic objective of accounting system is to record input in the form of transactions and generate output in the form of reports as shown in the Fig. 2.2.3.

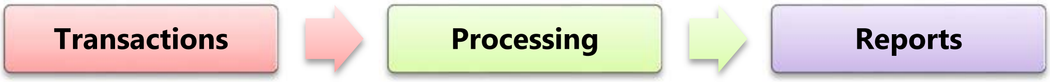


Fig. 2.2.3: Objective of Accounting System

Let us consider a simple transaction of capital introduction in business in cash ₹ 1,00,000. This transaction is recorded as under in Table 2.2.1.

Table 2.2.1: Data Sample Transaction

Receipt No.1	**Date: 01st Apr. 2017**	
Cash		Dr. 1,00,000
To Capital	Cr. 1,00,000	
Narration: (Being capital introduced in business)		

Above information is stored in Accounting Information Systems in two ways, in the form of **Master Data** and **Transaction Data**. Let us understand what is stored in the system through Table 2.2.2.

Table 2.2.2: Data Stored in Forms

Master Data	Non-Master Data
Voucher Type (i.e. Receipt Voucher in this case)	Voucher Number (i.e. 1 in this case)
Debit Ledger Name (i.e. Cash in this case)	Debit Ledger Amount (i.e. ₹1,00,000 in this case)
Credit Ledger Name (i.e. Capital in this case)	Credit Ledger Amount (i.e. ₹1,00,000 in this case)
	Date (i.e. 01st Apr. 2017 in this case)
	Narration

Please note:

- Master data is generally not typed by the user; it is selected from the available list. E.g. Debit Ledger name is selected from the available list of ledgers. If ledger is not created, user needs to create it first to complete the voucher entry.
- Master data entry is usually done less frequently say once a year or when there is a need to update. For example - prices are contracted with Vendors after deliberations and the agreed prices are updated in the Vendor master when new prices are negotiated. Generally, these are not done as frequently as the transactions with the Vendor itself. Effective controls over master data entry would be a 'four eye' check, where, there is another person who independently checks whether the master data entry is accurately done in the financial system of the company.
- Non-master data is typed by the user and not selected from available list as it is a non-permanent and it keeps on changing again and again.
- Sometimes transactional data could also be selected from a drop down list of inputs available to the user. For example, when a GRN (Goods Receipt Note) is created by the Stores/Warehouse personnel, they might only select the open purchase orders available in the system and input actual quantities received. In this case, many fields required to complete the transaction is pre-filled by the system and the user is not allowed to edit those fields.
- Master data is selected from the available list of masters (e.g. Ledgers) to maintain standardization as we need to collect all the transactions relating to one master data at one place for reporting. E.g. all cash transactions are collected in Cash Ledger for reporting purpose all transactions relating to capital are collected in Capital Ledger for reporting purpose.

- While inputting the information, user is forced to select master data from the available list just to avoid confusion while preparing reports. For example - same ledger name may be written differently.

II. Voucher Types

In accounting language, a **Voucher** is a documentary evidence of a transaction. There may be different documentary evidences for different types of transactions. E.g. Receipt given to a customer after making payment by him/her is documentary evidence of amount received. A sales invoice, a purchase invoice, is also a documentary evidence of transaction. Journal voucher is a documentary evidence of a non-cash/bank transaction. In accounting, every transaction, before it is recorded in the accounting system, must be supported by a documentary proof. In computer language, the word voucher has got a little different meaning. Voucher is a place where transactions are recorded. It is a data input form for inputting transaction data. In accounting, there may be different types of transactions; hence we use different voucher types for recording of different transactions. Generally following types of vouchers are used in accounting systems as shown in Table 2.2.3.

Table 2.2.3: Voucher Types

Module - Accounting		
S. No.	**Voucher Type**	**Use**
1	Contra	For recording of four types of transactions as under. a. Cash deposit in bank b. Cash withdrawal from bank c. Cash transfer from one location to another. d. Fund transfer from our one bank account to our own another bank account.
2	Payment	For recording of all types of payments. Whenever the money is going out of business by any mode (cash/bank).
3	Receipt	For recording of all types of receipts. Whenever money is being received into business from outside by any mode (cash/bank).
4	Journal	For recording of all non-cash/bank transactions. E.g. Depreciation, Provision, Write-off, Write-back, discount given/received, Purchase/Sale of fixed assets on credit, etc.

5	Sales	For recording all types of trading sales by any mode (cash/bank/credit).
6	Purchase	For recording all types of trading purchase by any mode (cash/bank/credit).
7	Credit Note	For making changes/corrections in already recorded sales/purchase transactions.
8	Debit Note	For making changes/corrections in already recorded sales/purchase transactions.
9	Memorandum	For recording of transaction which will be in the system but will not affect the trial balance.
Module -Inventory		
10	Purchase Order	For recording of a purchase order raised on a vendor.
11	Sales Order	For recording of a sales order received from a customer.
12	Stock Journal	For recording of physical movement of stock from one location to another.
13	Physical Stock	For making corrections in stock after physical counting.
14	Delivery Note	For recording of physical delivery of goods sold to a customer.
15	Receipt Note	For recording of physical receipt of goods purchased from a vendor.
Module - Payroll		
16	Attendance	For recording of attendance of employees.
17	Payroll	For salary calculations.

In some financial systems, instead of the word “Voucher”, the word “Document” is used. Above Table 2.2.3 shows an illustrative list of some of the voucher types. Different system may have some more voucher types. Also, user may create any number of new voucher types as per requirement. E.g. In Table 2.2.3, only “Payment” voucher type is mentioned. But user may create two different voucher types for making payment through two different modes, i.e. Cash Payment and Bank Payment.

III. Voucher Number

A **Voucher Number** or a **Document Number** is a unique identity of any voucher/document. A voucher may be identified or searched using its unique voucher number. Let us understand some peculiarities about voucher numbering.

- Voucher number must be unique.
- Every voucher type shall have a separate numbering series
- A voucher number may have prefix or suffix or both, e.g. ICPL/2034/17-18. In this case "ICPL" is the prefix, "17-18" is the suffix and "2034" is the actual number of the voucher.
- All vouchers must be numbered serially, i.e. 1,2,3,4,5,6 and so on.
- All vouchers are recorded in chronological order and hence voucher recorded earlier must have an earlier number, i.e. if voucher number for a payment voucher having date as 15thApril 2017 is 112, voucher number for all the vouchers recorded after this date shall be more than 112 only.

IV. Accounting Flow

In introduction part, we have discussed accounting flow from the angle of an accountant. Now we are going to discuss accounting flow from the angle of software.

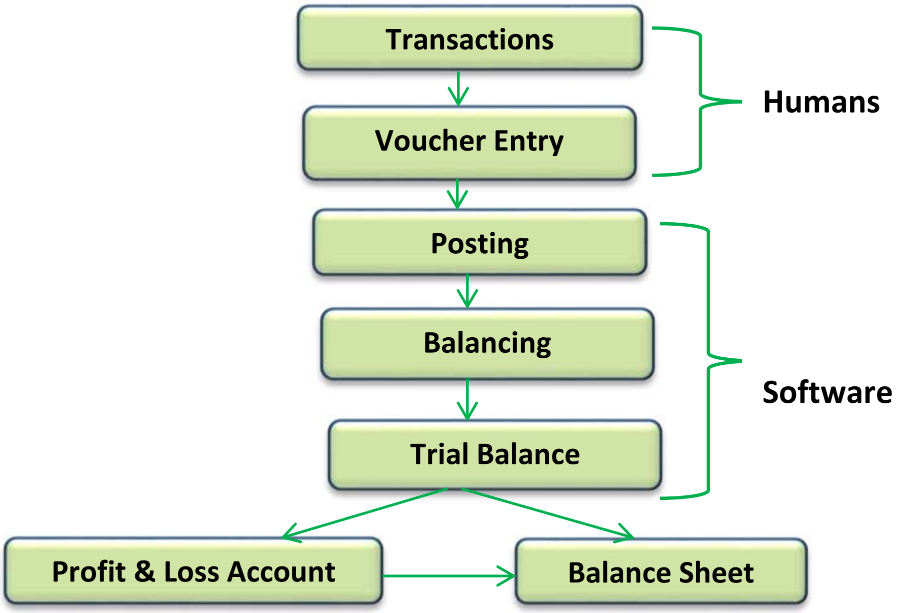


Fig. 2.2.4: Flow of Accounting

As shown in the Fig. 2.2.4 regarding the flow of accounting, in all there are seven steps in accounting flow, out of which only first two steps require human intervention. Remaining five steps are mechanical steps and can be performed by software with high speed and accuracy. Also, last five steps, i.e. Posting, Balancing, Trial Balance preparation, Profit and Loss Account preparation and Balance Sheet preparation are time consuming jobs and require huge efforts.

In very few cases, voucher entry may be automated and performed by software automatically. E.g. Interest calculation and application on monthly basis by a bank can be done by software automatically at the end of the month. But largely, voucher entry has to be done by a human being only.

V. Types of Ledgers

In accounting, we have studied that there are three types of ledger accounts, i.e. **Personal**, **Real** and **Nominal**. But as far as Financial and Accounting Systems are concerned, ledgers may be classified in two types only. Ledger having **Debit Balance** and ledger having **Credit Balance**. Why this is so? Let us understand with the help of the Fig. 2.2.5.

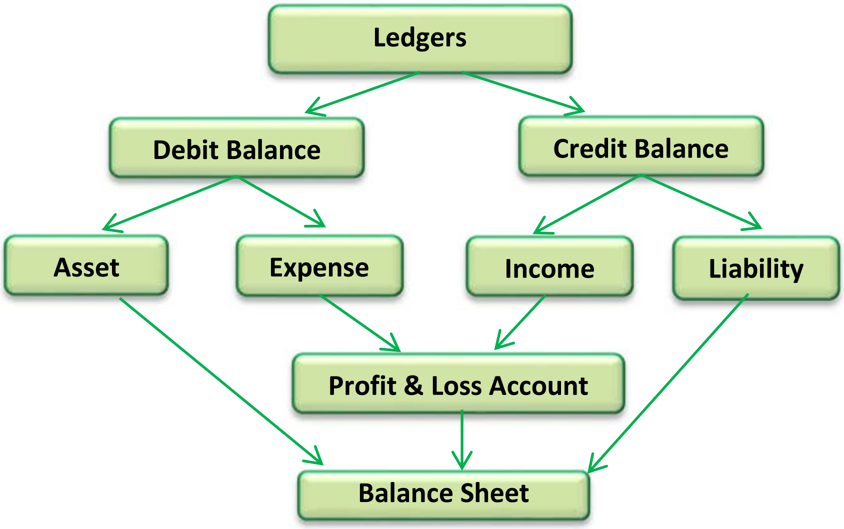


Fig. 2.2.5: Types of Ledgers

Please note –

- Basic objective of accounting software is to generate to two primary accounting reports, i.e. **Profit & Loss Account** and **Balance Sheet**. Income and Expense ledgers are considered in Profit & Loss Account and Asset and Liability ledgers are considered in Balance Sheet. Hence every ledger is classified in one of the four categories, i.e. Income, Expense, Asset or Liability.

- Difference between Total Income and Total Expenses, i.e. Profit or Loss as the case may be, is taken to Balance Sheet. So, everything in accounting software boils down to Balance Sheet. Balance Sheet is the last point in accounting process.
- Any ledger can be categorized in any one category only, i.e. Asset, Liability, Income or Expense. It cannot be categorized in more than one category.
- Ledger grouping is used for preparation of reports, i.e. Balance Sheet and Profit & Loss Account.

Accounting software does not recognize any ledger as Personal, Real or Nominal, instead it recognizes it as an Asset, Liability, Income or Expense Ledger.

VI. Grouping of Ledgers

At the time of creation of any new ledger, it must be placed under a particular group. There are four basic groups in Accounting, i.e. **Income**, **Expense**, **Asset**, **Liability**. There may be any number of sub groups under these four basic groups. Grouping is important as this is way to tell software what is the nature of the ledger and where it is to be shown at the time of reporting.

E.g. Cash ledger is an asset ledger and should be shown under current assets in Balance Sheet. If we group cash ledger under indirect expenses, it shall be displayed in profit and loss account as expenditure. Software cannot prevent incorrect grouping of ledger.

2.2.4 Technical Concepts

As now-a-days, almost all the Financial and Accounting Systems are computerized, it is necessary to understand how does it work? We are going to understand technical concepts from the perspective of a non-technical person or a layman who does not understand technicalities and does not want to go into technical details.

A. Working of any software (Refer Fig. 2.2.6)

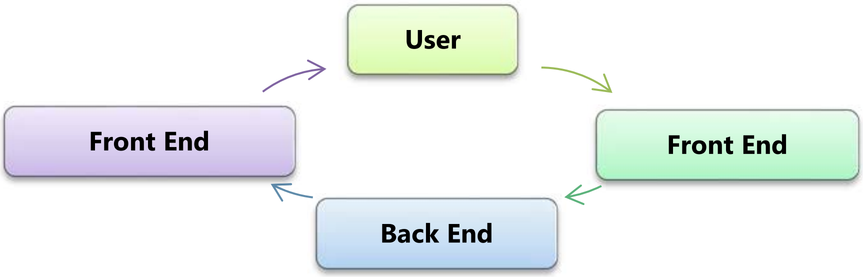


Fig. 2.2.6: Types of Ledgers

(i) Front End & Back End

These two words are used by software people again and again. Let us understand these two words in a simple language.

- **Front End** – It is part of the overall software which actually interacts with the user who is using the software.
- **Back End** – It is a part of the overall software which does not directly interact with the user, but interact with Front End only.

If a user wants to have some information from the system, i.e. Balance Sheet.

- User will interact with Front End part of the software and request front end to generate the report.
- Front End will receive the instruction from user and pass it on to the back end.
- Back End will process the data, generate the report and send it to the front end. Front end will now display the information to user.
- This is how the process gets completed each and every time.

To understand this concept in a better way, let us try to co-relate this with a situation in a restaurant as shown in the Fig. 2.2.7.

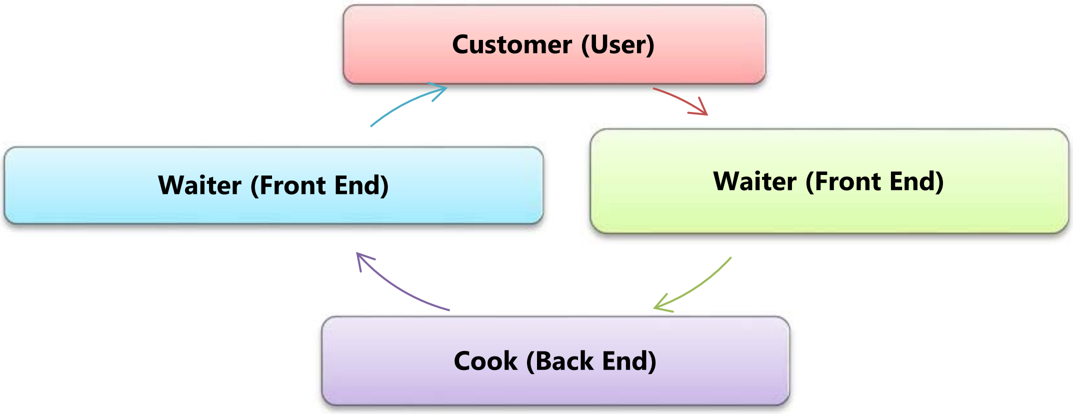


Fig. 2.2.7: An Illustrative Situation (For a customer in a Restaurant)

- A customer will place an order with waiter (Front End) and not with a cook (Back End) directly.
- Waiter will receive the order and pass it on to the cook in the kitchen.

- Cook will process the food as per requirement and had it over to the waiter.
- Waiter will serve the food to the customer.

(ii) Why separate Front End and Back End Software? Why not only one?

Reasons behind this can be summarized as under in the Table 2.2.4.

Table 2.2.4: Front End and Back End for Situation (cited in Fig. 2.2.7)

Reason	Restaurant	Software
Domain Expertise	A waiter is expert in handling customers; a cook is expert in cooking. These two jobs are separate and should not be mixed with each other. Both the jobs must be performed with topmost quality.	Front end software is meant for handling requests from users. Back end software is meant for storing and handling the data.
Presentation	Waiter can present himself as well as the food in a better way. Everybody likes good presentation. One cannot expect a good presentable cook as he/she works in kitchen.	Front end software interacting with a user is meant for presenting information in proper format, different colours, bold, italic letters, tables, charts, etc. Back end software is not meant for it and it can't be expected also.
User Experience	Waiter handles processed food and not raw material. Whole process of getting desired food from ordering to billing should be smooth and user experience should be very good. This is supposed to be done by well-trained waiter. This cannot be expected from a cook.	Front end software should guide a user to the desired report or feature. Front end software handles processed data and not raw data like back end. User interface of the front-end software needs to be intuitive, i.e. minimum use of help should be sought by user.
Speed	After placing an order, customer expects a quick delivery of food, nobody likes waiting period.	Using single software for both the aspects would unnecessarily increase the

	This is possible only with segregation of duties. Waiter will handle the customers only. Cook will keep on cooking only. Repeating the same activity again and again increases expertise and efficiency.	load and slow down the speed. Separate back end software is used for handling data only. This reduces the load and increases speed of operations.
Language	A waiter needs to be polished and polite. He/she needs to understand language of the customer and speak to the customer in the language in which the customer is comfortable. Cook must do nothing with this aspect as he is not interacting with customers. His job is to prepare best quality food only.	Front end speaks in the language understood by the user and understands language spoken by the Backend. Back end speaks in technical language not understood by a layman. Front end can speak in the languages, user's language and technical language.

(iii) Application Software

As already discussed in the previous chapter, application software performs many functions such as receiving the inputs from the user, interprets the instructions and performs logical functions so a desired output is achieved. Examples of application software would include SAP, Oracle Financials, MFG Pro etc.

In most software, there are three layers which together form the application namely; an **Application Layer**, an **Operating System Layer** and a **Database Layer**. This is called **Three Tier architecture**.

o The **Application Layer** receives the inputs from the users and performs certain validations like, if the user is authorized to request the transaction.

o The **Operating System Layer** then carries these instructions and processes them using the data stored in the database and returns the results to the application layer.

o The **Database Layer** stores the data in a certain form. For a transaction to be completed, all the three layers need to be invoked. Most application software is built on this model these days.

B. Installed Applications V/s Cloud-based Applications

(i) Using Software: These are the two ways (as shown in the Table 2.2.5) of using a software including Financial & Accounting Software.

- **Installed Applications:** These are programs that are installed on the hard disc of the user's computer.
- **Web Applications:** These are not installed on the hard disc of the user's computer, and are installed on a web server and accessed using a browser and internet connection. As technology and net connectivity improved virtually, all web based applications have moved to cloud based applications.
- ***Cloud Applications:*** ***These days many organizations do not want to install Financial Applications on their own IT infrastructure. For many organizations, the thought process is that it is not their primary function to operate complex IT systems and to have a dedicated IT team and hardware which requires hiring highly skilled IT resources and to maintain the hardware and software to run daily operations. The costs may become prohibitive. Thus, organizations increasingly are hosting their applications on Internet and outsource the IT functions. There are many methods through which this can be achieved. Most common among them being SaaS – Software as a Service or IaaS – Infrastructure as a Service.***

Table 2.2.5: Installed and Cloud Based Applications

Particulars	***Installed Application***	***Cloud Based Application***
Installation and Maintenance	***As software is installed on hard disc of the computer used by user, it needs to be installed on every computer one by one. This may take lot of time. Also, maintenance and updating of software may take lot time and efforts.***	***Installation on user computer is not required. Update and maintenance are defined responsibility of service provider.***
Accessibility	***As software is installed on the hard disc of the user's computer, user needs to go the computer only, i.e. the computer where software is installed, to use the software. It cannot be used from any***	***As software is available through online access, to use the software a browser and an internet connection is needed. It can be used from any computer in the world. Access to the software becomes very***

	computer.	easy. Also, it can be used 24 x 7.
Mobile Application	Using the software through mobile application is difficult in this case.	Mobile application becomes very easy as data is available 24x7. As technology evolves mobile technology is becoming an industry norm. That makes cloud based application future oriented.
Data Storage	Data is physically stored in the premises of the user, i.e. on the hard disc of the user's server computer. Hence user will have full control over the data.	Data is not stored in the user's server computer. It is stored on a web server. Ownership of data is defined in Service Level Agreement (SLA). SLA defines the rights, responsibilities and authority of both service provider and service user.
Data Security	As the data is in physical control of the user, user shall have the full physical control over the data and he/she can ensure that it is not accessed without proper access.	Data security is a challenge in case of cloud based application as the data is not in control of the user or owner of data. As time evolves; SLAs provides for details of back-up, disaster recovery alternatives being used by service provider.
Performance	A well written installed application shall always be faster than web application, reason being data is picked from local server without internet.	Access is dependent on speed of internet. Slow internet slows access to information and may slow operations.
Flexibility	It shall have more flexibility and controls as compared to web application. It is very easy to write desktop applications that take advantage of the user's hardware (such as: scanners, cameras, Wi-Fi, serial ports, network ports,	The success of cloud based applications is that they allow flexibility against both capital expenditure (CAPEX) and Operating Expense (OPEX) to the user. User can scale up operations as per need.

	etc.). Installed applications have this dis-advantage of higher capital expenditure (CAPEX) in comparison to cloud based application.	

2.2.5 Non-Integrated System

A **Non-Integrated System** is a system of maintaining data in a decentralized way. Each department shall maintain its own data separately and not in an integrated way. This is the major problem with non-integrated systems.

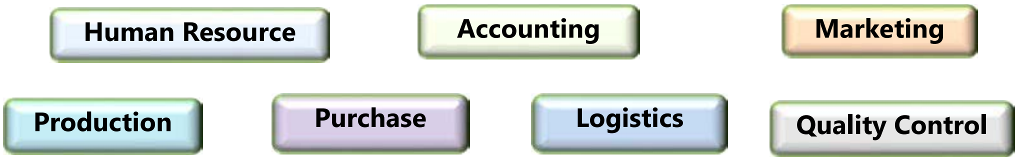


Fig. 2.2.8: Non-Integrated Systems

The Fig. 2.2.8 shows a typical non-integrated environment where all the departments are working independently and using their own set of data. They need to communicate with each but still they use their own data.

This results in two major problems:

a. Communication Gaps

b. Mismatched Data

Communication between different business units is a major aspect for success of any organization. Let us consider an example of mismatched master data. A customer record created by different departments for one customer named Ms. Jayshree Jadhao is shown in following Table 2.2.6 showing same customer name written differently.

Table 2.2.6: Same customer name written differently

Sr. No.	Name	Sr. No.	Name
1	JayashriJadhav	10	JayshriJadhaw
2	JayashreeJadhav	11	JayshreeJadhaw
3	JayshriJadhav	12	JayashriJadhao
4	JayshreeJadhav	13	JayashreeJadhao
5	JayashriJadhaw	14	JayshriJadhao
6	JayashreeJadhaw	15	JayshreeJadhao

7	JaishriJadhav	16	JaishreeJadhav
8	JaishriJadhao	17	JaishreeJadhao
9	JaishriJadhaw	18	JaishreeJadhaw

In the above case, we have considered first name and last name only. Had we used middle name also, few more permutations would have been possible. This may lead to total confusion in the organization at the time of inter-department communication.

2.2.6 Enterprise Resource Planning (ERP) Systems

It is an overall business management system that caters need of all the people connected with the organization. Every organization uses variety of resources in achieving its organization goals. ERP is an enterprise-wide information system designed to coordinate all the resources, information, and activities needed to complete business processes such as order fulfilment or billing.

Accounting and Finance function is considered as backbone for any business. Hence Financial & Accounting Systems are an important and integral part of ERP systems. ERP system includes so many other functions also. An ERP system supports most of the business system that maintains in a single database the data needed for a variety of business functions such as Manufacturing, Supply Chain Management, Financials, Projects, Human Resources and Customer Relationship Management.

An ERP system is based on a common database and a modular software design. The common database can allow every department of a business to store and retrieve information in real-time. The information should be reliable, accessible, and easily shared. The modular software design should mean a business can select the modules they need, mix and match modules from different vendors, and add new modules of their own to improve business performance.

Ideally, the data for the various business functions are integrated. In practice the ERP system may comprise a set of discrete applications, each maintaining a discrete data store within one physical database.

The term ERP originally referred to how a large organization planned to use organizational wide resources. In the past, ERP systems were used in larger more industrial types of companies. However, the use of ERP has changed and is extremely comprehensive, today the term can refer to any type of company, no matter what industry it falls in. In fact, ERP systems are used in almost any type of organization – large or small.

For a software system to be considered ERP, it must provide an organization with functionality for two or more systems. While some ERP packages exist that only cover two functions for an organization (QuickBooks: Payroll & Accounting), most ERP systems cover several functions.

Today's ERP systems can cover a wide range of functions and integrate them into one unified database. For instance, functions such as Human Resources, Supply Chain Management, Customer Relations Management, Financials, Manufacturing functions and Warehouse Management functions were all once stand-alone software applications, usually housed with their own database and network, today, they can all fit under one umbrella – the ERP system.

Some of the well-known ERPs in the market today include SAP, Oracle, MFG Pro, and MS Axapta etc.

Benefits of an ERP System

- ***<u>Information integration:</u> The reason ERP systems are called integrated is because they possess the ability to automatically update data between related business functions and components. For example - one needs to only update the status of an order at one place in the order-processing system; and all the other components will automatically get updated.***
- ***<u>Reduction of lead-time:</u> The elapsed time between placing an order and receiving it is known as the Lead-time. The ERP Systems by virtue of their integrated nature with many modules like Finance, Manufacturing, Material Management Module etc.; the use of the latest technologies like EFT (Electronic Fund Transfer), EDI (Electronic Data Interchange) reduce the lead times and make it possible for the organizations to have the items at the time they are required.***
- ***<u>On-time Shipment:</u> Since the different functions involved in the timely delivery of the finished goods to the customers- purchasing, material management production, production planning, plant maintenance, sales and distribution – are integrated and the procedures automated; the chances of errors are minimal and the production efficiency is high. Thus, by integrating the various business functions and automating the procedures and tasks the ERP system ensures on-time delivery of goods to the customers.***
- ***<u>Reduction in Cycle Time:</u> Cycle time is the time between placement of the order and delivery of the product. In an ERP System; all the data, updated to the minute, is available in the centralized database and all the***

procedures are automated, almost all these activities are done without human intervention. This efficiency of the ERP systems helps in reducing the cycle time.

- ***Improved Resource utilization:*** ***The efficient functioning of the different modules in the ERP system like manufacturing, material management, plant maintenance, sales and distribution ensures that the inventory is kept to a minimum level, the machine down time is minimum and the goods are produced only as per the demand and the finished goods are delivered to the customer in the most efficient way. Thus, the ERP systems help the organization in drastically improving the capacity and resource utilization.***

- ***Better Customer Satisfaction:*** ***Customer satisfaction means meeting or exceeding customers 'requirements for a product or service. With the help of web-enabled ERP systems, customers can place the order, track the status of the order and make the payment sitting at home. Since all the details of the product and the customer are available to the person at the technical support department also, the company will be able to better support the customer.***

- ***Improved Supplier Performance:*** ***ERP systems provide vendor management and procurement support tools designed to coordinate all aspects of the procurement process. They support the organization in its efforts to effectively negotiate, monitor and control procurement costs and schedules while assuring superior product quality. The supplier management and control processes are comprised of features that will help the organization in managing supplier relations, monitoring vendor activities and managing supplier quality.***

- ***Increased Flexibility:*** ***ERP Systems help the companies to remain flexible by making the company information available across the departmental barriers and automating most of the processes and procedures, thus enabling the company to react quickly to the changing market conditions.***

- ***Reduced Quality Costs:*** ***Quality is defined in many different ways-excellence, conformance to specifications, fitness for use, value for the price and so on. The ERP System's central database eliminates redundant specifications and ensures that a single change to standard procedures takes effect immediately throughout the organization. The ERP systems also provide tools for implementing total quality management programs within an organization.***

- ***Better Analysis and Planning Capabilities:*** ***Another advantage provided by ERP Systems is the boost to the planning functions. By enabling the comprehensive and unified management of related business functions such as production, finance, inventory management etc. and their data, it becomes possible to utilize fully many types of Decision Support Systems (DSS) and simulation functions, what-if analysis and so on; thus, enabling the decision-makers to make better and informed decisions.***

- ***Improved information accuracy and decision-making capability:*** ***The three fundamental characteristics of information are accuracy, relevancy and timeliness. The information needs to be accurate, relevant for the decision-maker and available to the decision-makers when he requires it. The strength of ERP Systems- integration and automation – help in improving the information accuracy and help in better decision-making.***

- ***Use of Latest Technology:*** ***ERP packages are adapted to utilize the latest developments in Information Technology such as open systems, client/server technology, Cloud Computing, Mobile computing etc. It is this adaptation of ERP packages to the latest changes in IT that makes the flexible adaptation to changes in future development environments possible.***

Fig. 2.2.9 showing different departments connecting with each other through central database.

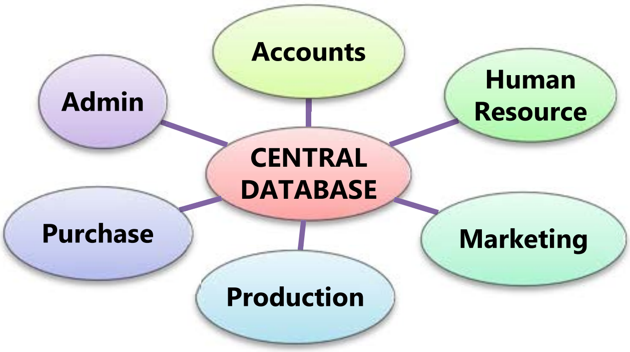


Fig. 2.2.9: Different Departments connected through Central Database

2.2.7 Features of an ERP System

An ERP System is that system which caters all types of needs of an organization and provides right data at right point of time to right users for their purpose. Hence, definition of ideal ERP system may change per organization. But generally, an ideal

ERP system is that system where a single database is utilized and contains all data for various software modules. These software modules can include the following:

- **Manufacturing:** Some of the functions include engineering, capacity, workflow management, quality control, bills of material, manufacturing process, etc.
- **Financials:** Accounts payable, accounts receivable, fixed assets, general ledger and cash management, etc.
- **Human Resources:** Benefits, training, payroll, time and attendance, etc.
- **Supply Chain Management:** Inventory, supply chain planning, supplier scheduling, claim processing, order entry, purchasing, etc.
- **Projects:** Costing, billing, activity management, time and expense, etc.
- **Customer Relationship Management (CRM):** CRM is a term applied to processes implemented by a company to handle its contact with its customers. CRM software is used to support these processes, storing information on current and prospective customers. Information in the system can be accessed and entered by employees in different departments, such as sales, marketing, customer service, training, professional development, performance management, human resource development, and compensation. Details on any customer contacts can also be stored in the system. The rationale behind this approach is to improve services provided directly to customers and to use the information in the system for targeted marketing.
- **Data Warehouse:** Usually this is a module that can be accessed by an organizations customers, suppliers and employees. Data warehouse is a repository of an organization’s electronically stored data. Data warehouses are designed to facilitate reporting and analysis. This classic definition of the data warehouse focuses on data storage. However, the means to retrieve and analyse data, to extract, transform and load data, and to manage the data dictionary are also considered essential components of a data warehousing system. An expanded definition for data warehousing includes business intelligence tools, tools to extract, transform, and load data into the repository, and tools to manage and retrieve metadata. In contrast to data warehouses are operational systems which perform day-to-day transaction processing. The process of transforming data into information and making it available to the user in a timely enough manner to make a difference is known as data warehousing.

Table 2.2.7 provides some examples of Free and Open Source ERP Software.

Table 2.2.7: Free and Open Source ERP software

S. No.	ERP Software	S. No.	ERP Software
1	Adempiere, a Java based ERP-System which started as a fork of Compiere	11	OpenBlueLab
2	Compiere, a Java based ERP-System	12	Openbravo, a Java based ERP-System
3	Dolibarr, a PHP based ERP system	13	OpenERP (formerly Tiny ERP)
4	ERP5, a Python based ERP system	14	Opentaps (Java based)
5	GNU Enterprise	15	OrangeHRM
6	GRR (software), a PHP/MySQL -based, web-accessed free ERP system	16	Postbooks from XTuple
7	JFire, a Java based ERP-System from NightLabs	17	SQL-Ledger
8	Kuali Foundation	18	Stoq
9	LedgerSMB	19	WebERP
10	OFBiz		

2.3 RISKS AND CONTROLS IN AN ERP ENVIRONMENT

Risk, its Management and related controls for various business processes have been discussed in detail in "Chapter – 1: Automated Business Processes" of the study material. The risks being discussed here are specific to ERP systems used.

2.3.1 Introduction

Major feature of an ERP System is **Central Database**. As the complete data is stored centrally at one place, ensuring safety of data and minimising risk of loss of data is a big challenge. In Non-Integrated System, data is stored by each department separately; hence this risk is low in such an environment. In an ERP environment, two major risks are faced by any organization:

- Due to central database, all the persons in an organization access the same set of data on a day to basis. This again poses the risk of leakage of information or access of information to non-related people. E.g. A person from sales department checking salary of a person in production.

- Again, as there is central database, all users shall use the same data for recording of transactions. Hence there is one more risk of putting incorrect data in the system by unrelated users. E.g. a person in Human Resource Department recording a purchase order. This is a risk due to central database only and controls are needed to minimise such type of risks.

2.3.2 ERP Implementation, its Risks and related Controls

ERP system implementation is a huge task and requires lot of time, money and above all patience. The success or failure of any ERP or saying it in terms of payback or ROI of an ERP, is dependent on its successful implementation and once implemented proper usage.

Tables 2.3.1(A,B,C,D,E) provide extensive discussion on the issues – People, Process, Technological, other implementation and post implementation issues that arise during implementation and related controls respectively.

1. People Issues: Employees, Management, implementation team, consultants and vendors – are the most crucial factor that decides the success or failure of an ERP System

Table 2.3.1(A): Risks and corresponding Controls related to People Issues

Aspect	***Risk Associated***	***Control Required***
Change Management	***Change will occur in the employee's job profile in terms of some jobs becoming irrelevant and some new jobs created.***	***Proper training of the users with well documented manuals. Practical hands on training of the ERP System should be provided so that the transition from old system to ERP system is smooth and hassle free.***
	The way in which organization functions will change, the planning, forecasting and decision-making capabilities will improve, information integration happening etc.	***It requires ensuring that a project charter or mission statement exists. The project requirements are to be properly documented and signed by the users and senior management.***
	Changing the scope of the project is another problem.	***This requires clear defining of change control procedures and holds everyone to them.***

Training	*Since the greater part of the raining takes place towards the end of the ERP implementation cycle, management may curtail the training due to increase in the overall cost budget.*	*Training is a project-managed activity and shall be imparted to the users in an organization by the skilled consultants and representatives of the hardware and package vendors.*
Staff Turnover	*As the overall system is integrated and connected with each other department, it becomes complicated and difficult to understand. Employee turnover – qualified and skilled personnel leaving the company - during the implementation and transition phases can affect the schedules and result in delayed implementation and cost overrun.*	*This can be controlled and minimized by allocation of employees to tasks matching their skill-set; fixing of compensation package and other benefits accordingly- thus keeping the employees happy and content and minimizing the staff turnover.*
Top Management Support	*ERP implementation will fail if the top management does not provide the support and grant permission for the availability of the huge resources that are required during the transition.*	*The ERP implementation shall be started only after the top management is fully convinced and assure of providing the full support.*
Consultants	*These are experts in the implementation of the ERP package and might not be familiar with the internal workings and organizational culture.*	*The consultants should be assigned a liaison officer - a senior manager – who can familiarize them with the company and its working.*

***<u>2. Process Risks:</u>* One of the main reason for ERP implementation is to improve, streamline and make the business process more efficient, productive and effective.**

Table 2.3.1(B): Risks and corresponding Controls related to Process Risks

Aspect	***Risk Associated***	***Control Required***
Program Management	***There could be a possibility of an information gap between day-to-day program management activities and ERP-enabled functions like materials and procurement planning, logistics and manufacturing.***	***This requires bridging the information gap between traditional ERP-based functions and high value operational management functions, such applications can provide reliable real-time information linkages to enable high-quality decision making.***
Business Process Reengineering (BPR)	***BPR means not just change – but dramatic change and dramatic improvements.***	***This requires overhauling of organizational structures, management systems, job descriptions, performance measurements, skill development., training and use of IT.***

3. Technological Risks: The organizations implementing ERP systems should keep abreast of the latest technological developments and implementation which is required to survive and thrive.

Table 2.3.1(C): Risks and corresponding Controls related to Technological Risks

Aspect	***Risk Associated***	***Control Required***
Software Functionality	***ERP systems offer a myriad of features and functions, however, not all organizations require those many features. Implementing all the functionality and features just for the sake of it can be disastrous for an organization.***	***Care should be taken to incorporate the features that are required by the organization and supporting additional features and functionality that might be required at a future date.***
Technological Obsolescence	***With the advent of more efficient technologies every day, the ERP system also becomes obsolete as time goes on.***	***This requires critical choice of technology, architecture of the product, ease of enhancements, ease of upgrading, quality of vendor support.***

Enhancement and Upgrades	*ERP Systems are not upgraded and kept up-to-date. Patches and upgrades are not installed and the tools are underutilised.*	*Care must be taken while selecting the vendor and upgrade/support contracts should be signed to minimize the risks.*
Application Portfolio Management	*These processes focus on the selection of new business applications and the projects required delivering them.*	*By bringing to the light the sheer number of applications in the current portfolio, IT organizations can begin to reduce duplication and complexity.*

4. Other Implementation Issues: ***Many times, ERP implementations are withdrawn because of the following factors.***

Table 2.3.1(D): Risks and corresponding Controls related to some other implementation issues

Aspect	*Risk Associated*	*Control Required*
Lengthy implementation time	*ERP projects are lengthy that takes anywhere between 1 to 4 years depending upon the size of the organization. Due to technological developments happening every day, the business and technological environment during the start and completion of the project will never be the same. Employee turnover is another problem.*	*Care must be taken to keep the momentum high and enthusiasm live amongst the employees, so as to minimize the risk.*
Insufficient Funding	*The budget for ERP implementation is generally allocated without consulting experts and then implementation is stopped along the way, due to lack of funds.*	*It is necessary to allocate necessary funds for the ERP implementation project and then allocate some more for contingencies.*
Data Safety	*As there is only one set of data, if this data is lost, whole business may come to stand still.*	*Back up arrangement needs to be very strong. Also, strict physical control is needed for data.*

Speed of Operation	As data is maintained centrally, gradually the data size becomes more and more and it may reduce the speed of operation.	This can be controlled by removing redundant data, using techniques like data warehousing and updating hardware on a continuous basis.
System Failure	As everybody is connected to a single system and central database, in case of failure of system, the whole business may come to stand still may get affected badly.	This can be controlled and minimized by having proper and updated back up of data as well as alternate hardware / internet arrangements. In case of failure of primary system, secondary system may be used.
Data Access	Data is stored centrally and all the departments access the central data. This creates a possibility of access to non-relevant data.	Access rights need to be defined very carefully and to be given on "Need to know" and Need to do" basis only.

5. Post Implementation issues: ERP operation and maintenance requires a lifelong commitment by the company management and users of the system.

Table 2.3.1(E): Risks and corresponding Controls related to post-implementation issues

Aspect	Risk Associated	Control Required
Lifelong commitment	Even after the ERP implementation, there will always be new modules/versions to install, new persons to be trained, new technologies to be embraced, refresher courses to be conducted and so on.	This requires a strong level of commitment and consistency by the management and users of the system.

2.3.3 Role Based Access Control (RBAC) in ERP System

In computer systems security, **Role-Based Access Control** is an approach to restricting system access to authorized users. It is used by most enterprises and can implement mandatory access control or discretionary access control. RBAC, sometimes referred to as Role-Based Security, is a policy neutral access control mechanism defined around roles and privileges that lets employees having access rights only to the information they need to do their jobs and prevent them from accessing information that doesn't pertain to them. The components of RBAC such as role-permissions, user-role and role-role relationships make it simple to perform user assignments. RBAC can be used to facilitate administration of security in large organizations with hundreds of users and thousands of permissions.

Roles for staff are defined in organization and permission to access a specific system or perform certain operation is defined as per the role assigned. E.g. a junior accountant in accounting department is assigned a role of recording basic accounting transactions, an executive in human resource department is assigned a role of gathering data for salary calculations on monthly basis, etc.

D. Types of Access

While assigning access to Master Data, Transaction Data and Reports to different users; following options are possible.

(i) **Create** – Allows to create data;

(ii) **Alter** – Allows to alter data;

(iii) **View** – Allows only to view data; and

(iv) **Print** – Allows to print data

Let us consider a small case study for better understanding of Role Based Access and Controls in Financial and Accounting Systems. Indradhanu Consulting Private Limited, a company dealing in project management is having different users as given in the Table 2.3.2 under.

Table 2.3.2: Users Database of Indradhanu Consulting Private Limited (Illustrative)

S. No.	Employee Name	Designation	Allow Access To	Dis-allow access to
1	Swapnil Ghate	Director	Complete access to all the reports, masters and	Creation / Alteration

			transactions but limited to viewing purpose only. No need to give any alteration or creation access.	
2	CA. Pankaj Deshpande	CFO	Same as director but in some cases, creation or alteration access to masters and transactions may be given.	
3	Mayura Rahane	Head HR	Full access to all HR related masters and transactions, e.g. Creation and alteration of employees, pay heads, salary structures, leave types etc. Creation and alteration of leave and salary calculations etc.	All non-related masters, transactions and reports.
4	Amit Shriwas	Head-Accounts	Full access to all accounting masters, transactions and reports.	All non-related masters, transactions and reports.
5	Sachi Dongre	Accountant	Only voucher entry and viewing accounting master data.	Reports like Balance Sheet, Profit & Loss access to ledger creation or alteration.
6	Tanushree Daware	Head-Marketing	Fully access to customer master data, transaction history, purchase habits of customers may be given. Only view access for sales data.	All non-related masters, transactions and reports.
7	Sujay Kalkotwar	Manager-Taxation	Full access to taxation reports, tax related transactions, Access to Balance Sheet and Profit & Loss Account is also needed as tax figures affect these reports.	All non-related masters, transactions and reports.
8	Aditi Kurhekar	Head-Purchases	Full Access to Purchase Order, Goods Receipt Note and Purchase Vouchers should be	All non-related masters, transactions and

			given. View access to vendor master data is also needed.	reports.
9	Gayatri Rathod	Data Entry Operator	Very limited access should be given.	Access to accounting master data creation or alteration, access to reports like balance sheet, profit & loss accounts.
10	Sanjay Somkuwar	Cashier	Cash payment and cash receipt vouchers only.	All master and transaction data (other than cash), Backdated voucher entry.
11	Surbhee Chincholkar	Stores Incharge	Creation, Alteration of Inventory master data, Inventory transactions, Inventory reports, etc.	All non-related masters, transactions and reports.

2.4 AUDIT OF ERP SYSTEMS

The fundamental objectives of an audit of controls do not change in an ERP environment. When evaluating controls over ERP systems, decisions must be made regarding the relevance of operational internal control procedures to Information Technology (IT) controls. Specific control procedures for audit objectives must be tested.

ERP systems should produce accurate, complete, and authorized information that is supportable and timely. In a computing environment, this is accomplished by a combination of controls in the ERP System, and controls in the environment in which the ERP system operates, including its operating system. Controls are divided into **General Controls** and **Application Controls**.

♦ **General Controls** include controls over Information Technology management controls addressing the information technology oversight process; Information Technology infrastructure, security management and software acquisition; monitoring and reporting information technology activities; business improvement initiatives; and development and maintenance. These controls apply to all systems – from mainframe to client/server to desktop computing environments. General controls can be further divided into **Management Controls** and **Environmental Controls**.

- **Management Controls** deal with organizations, policies, procedures, planning, and so on.
- **Environmental Controls** are the operational controls administered through the computer centre/computer operations group and the built-in operating system controls.

♦ **Application Controls** pertain to the scope of individual business processes or application systems. Individual applications may rely on effective operation of controls over information systems to ensure that interface data are generated when needed, supporting applications are available and interface errors are detected quickly.

Some of the questions auditors should ask during an ERP audit are pretty much the same as those that should be asked during development and implementation of the system:

♦ Does the system process as per GAAP (Generally Accepted Accounting Principles) and GAAS (Generally Accepted Auditing Standards)?

♦ Does it meet the needs for reporting, whether regulatory or organizational?

♦ Were adequate user requirements developed through meaningful interaction?

♦ Does the system protect confidentiality and integrity of information assets?

♦ Does it have controls to process only authentic, valid, accurate transactions?

♦ Are effective system operations and support functions provided?

♦ Are all system resources protected from unauthorized access and use?

♦ Are user privileges based on what is called "role-based access?"

♦ Is there an ERP system administrator with clearly defined responsibilities?

♦ Is the functionality acceptable? Are user requirements met? Are users happy?

♦ Have workarounds or manual steps been required to meet business needs?

♦ Are there adequate audit trails and monitoring of user activities?

♦ Can the system provide management with suitable performance data?

♦ Are users trained? Do they have complete and current documentation?

♦ Is there a problem-escalation process?

Auditing aspects in case of any ERP system can be summarized as under:

(i) Auditing of Data

- **Physical Safety** – Ensuring physical control over data.
- **Access Control** – Ensuring access to the system is given on "need to know" (a junior accountant need not view Profit & Loss Account of the business) and "need to do basis" (HR executive need not record a Purchase Order).

(ii) Auditing of Processes

- **Functional Audit –** This includes testing of different functions / features in the system and testing of the overall process or part of process in the system and its comparison with actual process. E.g. Purchase Process, Sales Process, Salary Calculation Process, Recruitment Process, etc. Auditor may check this process in the system and compare it with actual process. It is quite possible that all the aspect present in the actual process may not be integrated in the ERP system. There may be some manual intervention.
- **Input Validations –** This stands for checking of rules for input of data into the system. E.g. a transaction of cash sales on sales counter must not be recorded in a date other than today (not a future date or a back date), amount field must not be zero, stock item field shall not be empty, etc. Input validations shall change according to each data input form.

2.5 ERP CASE STUDY OF A CHARTERED ACCOUNTANT FIRM

As everybody is familiar with working environment in a Chartered Accountant (CA) firm let us consider possibility of implementing ERP system in a CA Firm.

Case 1 - Nirman Infrastructures Pvt. Ltd. a client of Ghate Deshpande & Co. (a CA Firm) receives a notice for scrutiny assessment from Income Tax Department. Following shall be the events in normal case.

(i) Client informs about receipt of notice to CA. Pankaj Deshpande (Partner) on phone and sends the copy of notice to CA Firm.

(ii) Notice is received at CA firm, read and understood. A task for giving reply to Income Tax Department is allotted to Sachi Dongre, an article clerk.

(iii) Sachi asks for some original documents (PAN, Memorandum of Articles, Agreements etc.) from client for working. These documents need to be returned to client after the work.

(iv) Sachi works on this task, prepares the reply and submits it with Income Tax Department. Also, he updates CA. Pankaj Deshpande and Mayura (Accountant) about it.

(v) Bill is prepared by Mayura and approved by CA. Pankaj Deshpande.

(vi) Bill is submitted with client.

(vii) Documents are returned to client.

(viii) Cheque received from client against the bill submitted.

(ix) Receipt is recorded in books of accounts.

This is how a simple case is handled in a CA Firm. Let us now discuss important points regarding this case.

In case of any ERP System, two aspects are very important – Communication (Internal and External) and Documentation.

Example - CA Firm Work Flow using Integrated System (Refer Fig. 2.5.1)

- Communication in this case is starting from client.
- Instead of client calling his CA, he should put the information as a service request in the central database maintained by CA Firm.
- As soon as service request is put by client into the system, one or more partner should be informed by the system about new service request.
- Partner shall convert this request into the task and allot it to one of the assistant.
- On allotment of task to the assistant, client must be updated about this task allotment.
- Article assistant shall contact client for requirement of information regarding work.
- Client shall submit the document through the system and update the information in central database.

- Article shall complete the work and send it for approval of his boss.
- After approval of work by article, client shall be automatically informed about it through the system only.
- Information shall be passed on to accounts department for preparation of bill for this assignment.
- Bill shall be raised from the system and sent to client through email.
- Client shall pay the fees and receipt is recorded in the same system.

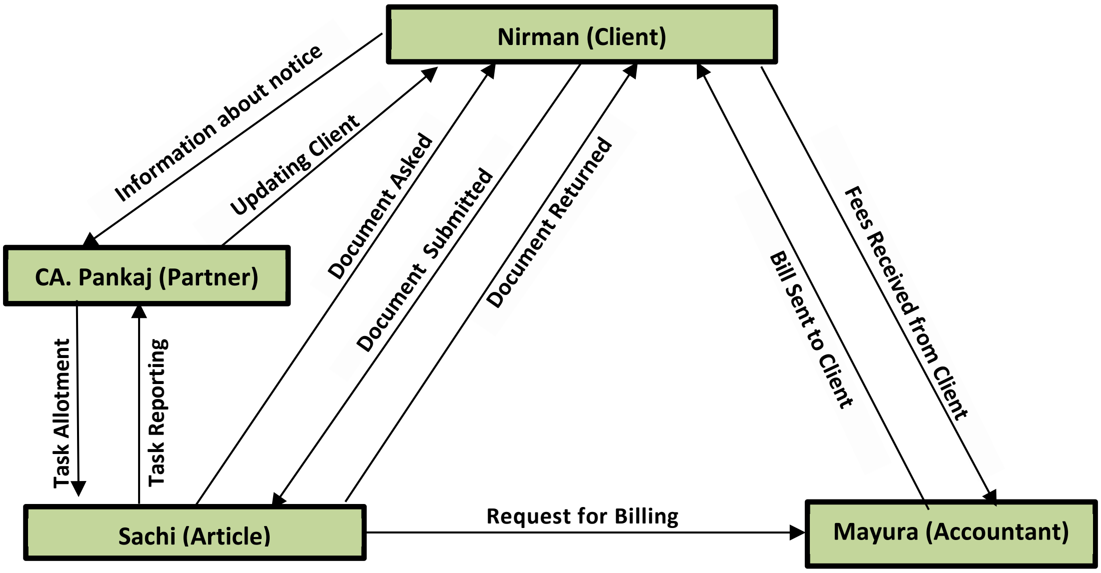


Fig. 2.5.1: CA Firm Work Flow

In this whole process, two important aspects, i.e. Communication and Documentation are taken care of in the best possible manner. Instead of a person communicating with other, system is communicating automatically after every updation. Fig. 2.5.2 showing different people connected to central database.

In case of Integrated System, there shall be only one system of communication with others. But in case of non-integrated system people use multiple modes for communication like making a phone call, sending SMS, Email, WhatsApp or personal meeting. But the major problem with these multiple option is that there is no inter-connectivity between these modes and hence track of the overall process is not available.

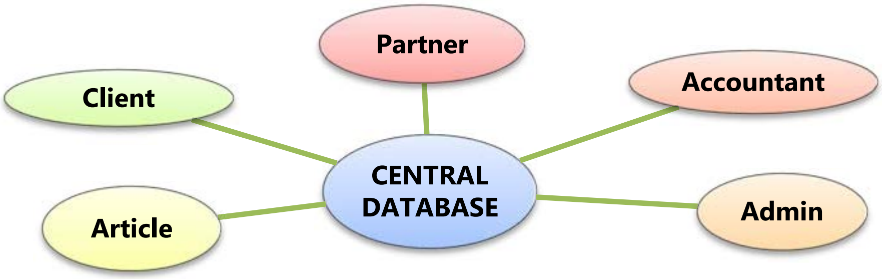


Fig. 2.5.2: Different people connected to Central Database

2.6 BUSINESS PROCESS MODULES AND THEIR INTEGRATION WITH FINANCIAL AND ACCOUNTING SYSTEMS

2.6.1 What is a Business Process?

A **Business Process** consists of a set of activities that are performed in coordination in an organizational and technical environment. These activities jointly realize a business goal. Each business process is enacted by a single organization, but it may interact with business processes performed by other organizations. To manage a process-

- The first task is to **define** it. This involves defining the steps (tasks) in the process and mapping the tasks to the roles involved in the process.
- Once the process is mapped and implemented, **performance measures** can be established. Establishing measurements creates a basis to improve the process.
- The last piece of the process management definition describes the **organizational setup** that enables the standardization of and adherence to the process throughout the organization. Assigning enterprise process owners and aligning employees' performance reviews and compensation to the value creation of the processes could accomplish this.

Process management is based on a view of an organization as a system of interlinked processes which involves concerted efforts to map, improve and adhere to organizational processes. Whereas traditional organizations are composed of departments and functional stages, this definition views organizations as networks or systems of processes. Process orientation is at the core of BPM.

2.6.2 Business Process Flow

As discussed earlier, a **Business Process** is a prescribed sequence of work steps performed to produce a desired result for the organization. A business process is initiated by a kind of event, has a well-defined beginning and end, and is usually completed in a relatively short period. Organizations have many different business processes such as completing a sale, purchasing raw materials, paying employees and paying vendors, etc. Each of the business processes has either a direct or indirect effect on the financial status of the organization. The number and type of business processes and how the processes are performed would vary across enterprises and is also impacted by automation. However, most of the common processes would flow a generic life cycle.

For Example: Accounting Process Flow

Accounting or Book keeping cycle covers the business processes involved in recording and processing accounting events of a company. It begins when a transaction or financial event occurs and ends with its inclusion in the financial statements. A typical life cycle of an accounting transaction may include the following transactions as depicted in Fig. 2.6.1:

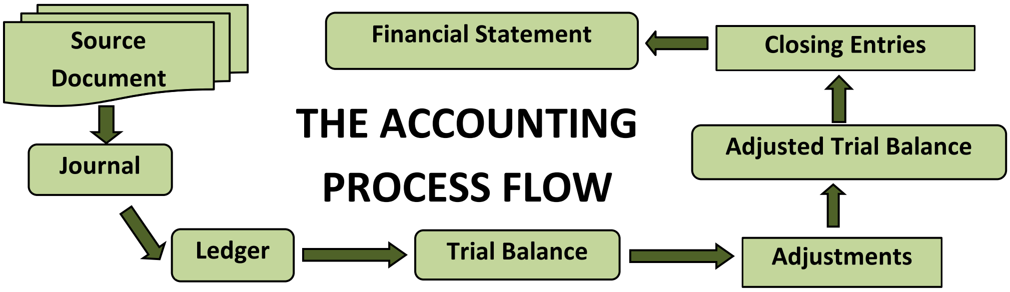


Fig. 2.6.1: Accounting Process Flow

(a) **Source Document:** A document that captures data from transactions and events.

(b) **Journal:** Transactions are recorded into journals from the source document.

(c) **Ledger:** Entries are posted to the ledger from the journal.

(d) **Trial Balance:** Unadjusted trial balance containing totals from all account heads is prepared.

(e) **Adjustments:** Appropriate adjustment entries are passed.

(f) **Adjusted Trial balance:** The trial balance is finalized post adjustments.

(g) **Closing Entries:** Appropriate entries are passed to transfer accounts to financial statements.

(h) **Financial statement:** The accounts are organized into the financial statements.

Many examples like Order to Cash Process Flow (O2C), Procure to Pay Process Flow (P2P) have already been discussed in detail in Chapter 1.

2.6.3 ERP - Business Process Modules (BPM)

A. Business Categories of BPM

There are three different nature and types of businesses that are operated with the purpose of earning profit. Each type of business has distinctive features.

- **Trading Business –** Trading simply means buying and selling goods without any modifications, as it is. Hence inventory accounting is a major aspect in this case. Purchase and sales transactions cover major portion of accounting. This industry requires accounting as well as inventory modules.
- **Manufacturing Business –** This type of business includes all aspects of trading business plus additional aspect of manufacturing. Manufacturing is simply buying raw material, changing its form and selling it as a part of trading. Here also, inventory accounting plays a major role. This type of industry requires accounting and complete inventory along with manufacturing module.
- **Service Business –** This type of business does not have any inventory. It is selling of skills/knowledge/Efforts/time. Eg: Doctors, Architects, Chartered Accountants, are the professionals into service business. There may be other type of business into service, i.e. courier business, security service, etc. This industry does not require inventory module.

B. Functional Modules of ERP

Business process may change per type of business. There may be different business units within a business. Hence different modules are possible in an integrated system. There may be modules as under. Fig. 2.6.2 shows different business process modules in ERP System. There may be some other modules also. Different types of industries require different modules.

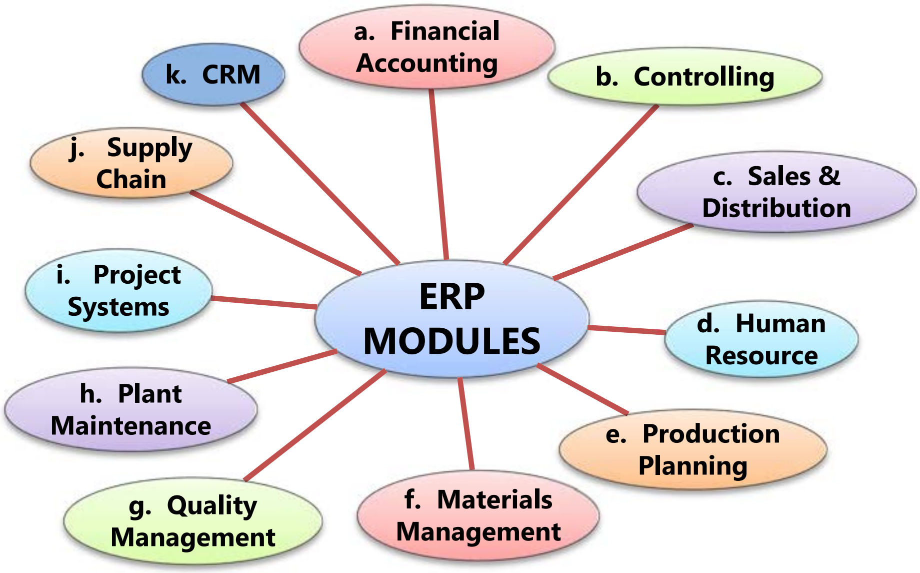


Fig. 2.6.2: ERP Modules

a. Financial Accounting Module

This module is the most important module of the overall ERP System and it connects all the modules to each other. Every module is somehow connected with module. Following are the key features of this module.

- Tracking of flow of financial data across the organization in a controlled manner and integrating all the information for effective strategic decision making.
- Creation of Organizational Structure (Defining Company, Company Codes, business Areas, Functional Areas, Credit Control, Assignment of Company Codes to Credit Controls).
- Financial Accounting Global Settings (Maintenance of Fiscal Year, Posting Periods, defining Document types, posting keys, Number ranges for documents).
- General Ledger Accounting (Creation of Chart of Accounts, Account groups, defining data transfer rules, creation of General Ledger Account).
- Tax Configuration & Creation and Maintenance of House of Banks.

- ♦ Account Payables (Creation of Vendor Master data and vendor-related finance attributes like account groups and payment terms).
- ♦ Account Receivables (Creation of Customer Master data and customer-related finance attributes like account groups and payment terms.
- ♦ Asset Accounting.
- ♦ Integration with Sales and Distribution and Materials Management.

b. Controlling Module

This module facilitates coordinating, monitoring, and optimizing all the processes in an organization. It controls the business flow in an organization. This module helps in analysing the actual figures with the planned data and in planning business strategies. Two kinds of elements are managed in Controlling Module –**Cost Elements** and **Revenue Elements**. These elements are stored in the Financial Accounting module.

<u>Key features of this module are as under:</u>

- ***<u>Cost Element Accounting:</u> This component provides overview of the costs and revenues that occur in an organization. The cost elements are the basis for cost accounting and enable the user the ability to display costs for each of the accounts that have been assigned to the cost element. Examples of accounts that can be assigned are Cost Centres, Internal Orders, WBS (work breakdown structures).***
- ***<u>Cost Centre Accounting:</u> This provides information on the costs incurred by the business. Cost Centres can be created for such functional areas as Marketing, Purchasing, Human Resources, Finance, Facilities, Information Systems, Administrative Support, Legal, Shipping/Receiving, or even Quality. Some of the benefits of Cost Centre Accounting are that the managers can set budget/cost Centre targets; Planning; Availability of Cost allocation methods; and Assessments/Distribution of costs to other cost objects.***
- ***<u>Activity-Based-Accounting:</u> This analyse cross-departmental business processes and allows for a process-oriented and cross-functional view of the cost centres.***
- ***<u>Internal Orders:</u> Internal Orders provide a means of tracking costs of a specific job, service, or task. These are used as a method to collect those costs and business transactions related to the task. This level of monitoring can be very detailed but allows***

management the ability to review Internal Order activity for better-decision making purposes.

- ***<u>Product Cost Controlling:</u> This calculates the costs that occur during the manufacture of a product or provision of a service and allows the management the ability to analyse their product costs and to make decisions on the optimal price(s) to market their products.***
- ***<u>Profitability Analysis:</u> This allows the management to review information with respect to the company's profit or contribution margin by individual market segment.***
- ***<u>Profit Centre Accounting:</u> This evaluates the profit or loss of individual, independent areas within an organization.***

c. Sales and Distribution Module

Sales and Distribution is one of the most important modules. It has a high level of integration complexity. Sales and Distribution is used by organizations to support sales and distribution activities of products and services, starting from enquiry to order and then ending with delivery.

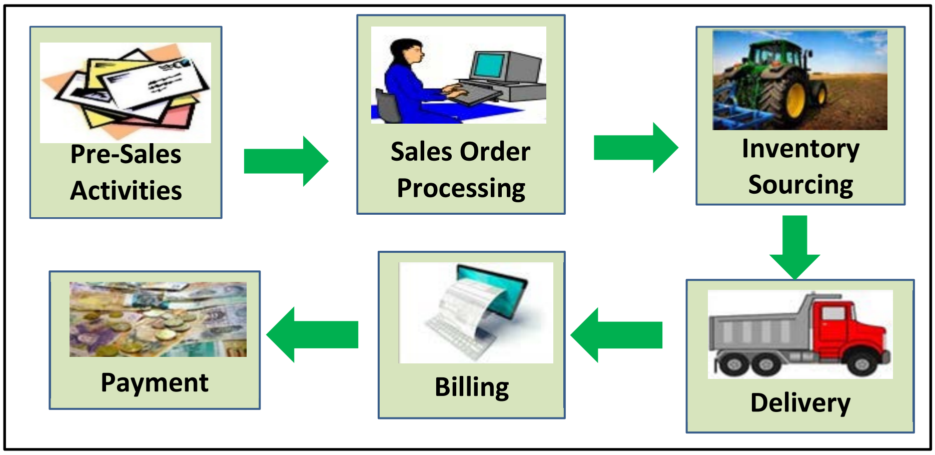


Fig. 2.6.3: Sales and Distribution with ERP

Sales and Distribution can monitor a plethora of activities that take place in an organization such as products enquires, quotation (pre-sales activities), placing order, pricing, scheduling deliveries (sales activity), picking, packing, goods issue, shipment of products to customers, delivery of products and billings. In all these processes, multiple modules are involved such as FA (Finance & Accounting), CO (Controlling), MM (Material Management), PP (Production Planning), LE (Logistics Execution), etc.; which shows the complexity of the integration involved.

Key features of Sales and Distribution Module are discussed as under:

- **Setting up Organization Structure:** Creation of new company, company codes, sales organization, distribution channels, divisions, business area, plants, sales area, maintaining sales offices, storage location;
- **Assigning Organizational Units:** Assignment of individual components created in the above activities with each other per design like company code to company, sales organization to company code, distribution channel to sales organization, etc.;
- **Defining Pricing Components:** Defining condition tables, condition types, condition sequences;
- Setting up sales document types, billing types, and tax-related components; and
- Setting up Customer master data records and configuration.

Sales and Distribution Process (Referring Fig. 2.6.3)

- **Pre-Sales Activities:** Include prospecting of customers, identifying prospective customers, gathering data, contacting them and fixing appointments, showing demo, discussion, submission of quotations, etc.
- **Sales Order:** Sales order is recorded in our books after getting a confirmed purchased order from our customer. Sales order shall contain details just like purchase order. E.g. Stock Item Details, Quantity, Rate, Due Date of Delivery, Place of Delivery, etc.
- **Inventory Sourcing:** It includes making arrangements before delivery of goods; ensuring goods are ready and available for delivery.
- **Material Delivery:** Material is delivered to the customer as per sales order. All inventory details are copied from Sales Order to Material Delivery for saving user's time and efforts. This transaction shall have a linking with Sales Order. Stock balance shall be reduced on recording of this transaction.
- **Billing:** This is a transaction of raising an invoice against the delivery of material to customer. This transaction shall have a linking with Material Delivery and all the details shall be copied from it. Stock balance shall not affect again.
- **Receipt from Customer/Payment:** This is a transaction of receiving amount from customer against sales invoice and shall have a linking with sales invoice.

d. Human Resource Module

This module enhances the work process and data management within HR department of enterprises. Right from hiring a person to evaluating one's performance, managing promotions, compensations, handling payroll and other related activities of an HR is processed using this module. The task of managing the details and task flow of the most important resource i.e. human resource is managed using this module.

The most important objective of master data administration in Human Resources is to enter employee-related data for administrative, time-recording, and payroll purposes. Payroll and Personnel departments deal with Human Resource of the organization. This department maintains total employee database. Wage and attendance related information comes to this department. They also prepare wage sheet for workmen; handle Provident Fund, ESI related formalities. This is perhaps the only module, which exchange very few information with other modules.

Concerning manpower, its requirement and utilization is one of the major chunks of profit for an organization. So, in this regard, every aspect of business transaction is taken care of by defining the master shifts master, PF ESI (Employees' State Insurance) master, leave, holiday, loans, employee master, operations and sub-operations masters etc. Also, the various input transaction such as Attendance Entry, Leave, holiday, Earning/Deduction entry, Advances etc. Finally, different types of Payroll reports, which can be of various types according to specified company standard. Fig. 2.6.4 showing processes involved in Human Resource Department.

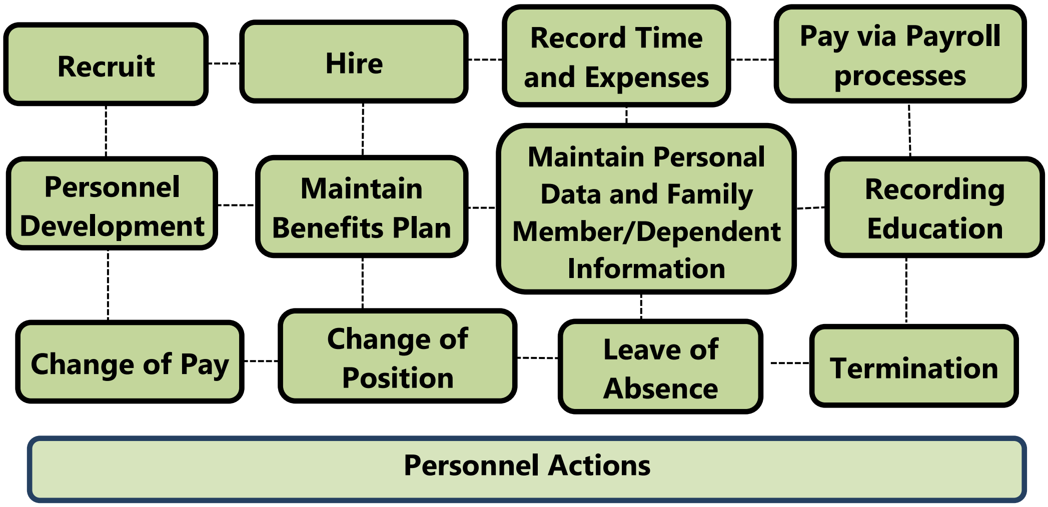


Fig. 2.6.4: Process in Human Resource Department

- The module starts with the employee and workmen master.

- Employees being a part of a department so there will be provision of department and designation master. The job of this module is to record the regular attendance of every employee.
- Usage of magnetic card or finger print recognition devices will help to improve the attendance system and provide an overall security in terms of discarding proxy attendance.
- Moreover, if the attendance related information can be digitised then the major portion of monthly salary can be automated. But the authority should study the feasibility of this kind of system.
- This module will also deal with the financial entries like advance or loan to employees.
- From Holiday master provided with the module, the user could feed all possible holidays at the beginning of a year, so leave related information can be automated. This module will generate monthly wage sheet from which the salary payment can be made and respective accounts will be updated.
- All figures will be protected under password. Only authorized person will be eligible to access information from this module

e. Production Planning (PP) Module

Production Planning (PP) Module is another important module that includes software designed specifically for production planning and management. This module also consists of master data, system configuration and transactions to accomplish plan procedure for production. PP module collaborates with Master Data, Sales and Operations Planning (SOP), Distribution Resource Planning (DRP), Production Planning, Material Requirements Planning (MRP), Capacity Planning, Product Cost Planning and so on while working towards production management in enterprises.

- ***Master Data*** ***– This includes the material master, work centres, routings and bill of materials.***
- ***SOP*** ***- Sales and Operations Planning (SOP) provides the ability to forecast sales and production plans based on historical, current and future data.***
- ***DRP*** ***- Distribution Resource Planning (DRP) allows companies the ability to plan the demand for distribution centres.***

- ***Production Planning* – This includes material forecasting, demand management, long term planning and master production scheduling (MPS).**
- ***MRP* - Material Requirements planning relies on demand and supply elements with the calculation parameters to calculate the net requirements from the planning run.**
- ***Capacity Planning* – This evaluates the capacity utilized based on the work centres available capacity to show capacity constraints.**
- ***Product Cost Planning* – This is the process of evaluating all the time values and value of component materials to determine the product cost.**

Fig. 2.6.5 discusses Production Planning Module.

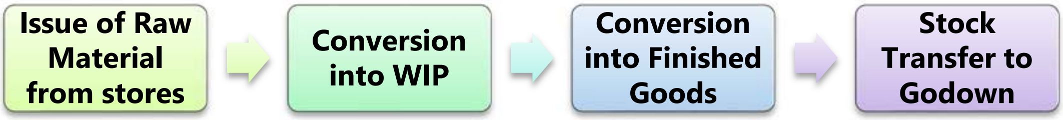

Issue of Raw Material from stores
Conversion into WIP
Conversion into Finished Goods
Stock Transfer to Godown

Fig. 2.6.5: Process in Production Planning Module

Conversion into Work In Process (WIP) may include more than one step. Also, conversion into Finished Goods may include packing process also.

f. Material Management (MM) Module

Material Management (MM) Module as the term suggests manages materials required, processed and produced in enterprises. Different types of procurement processes are managed with this system. Some of the popular sub-components in MM module are vendor master data; consumption based planning, purchasing, inventory management, invoice verification and so on. Material Management also deals with movement of materials via other modules like logistics, Supply Chain Management, sales and delivery, warehouse management, production and planning. Fig. 2.6.6 showing overall purchase process.

- **Purchase Requisition from Production Department:** Production department sends a request to purchase department for purchase of raw material required for production.
- **Evaluation of Requisition:** Purchase department shall evaluate the requisition with the current stock position and purchase order pending position and shall decide about accepting or rejection the requisition.
- **Asking for Quotation:** If requisition is accepted, quotations shall be asked to approve vendors for purchase of material.

- **Evaluation of Quotations:** Quotations received shall be evaluated and compared.
- **Purchase Order:** This is a transaction for letting an approved vendor know what we want to purchase, how much we want to purchase, at what rate we want to purchase, by what date we want the delivery, where we want the delivery. Hence a typical purchase order shall have following information.
  - Description of **stock items** to be purchased.
  - **Quantity** of these stock items.
  - **Rate** for purchases.
  - **Due Date** by which material is to be received.
  - **Godown** where material is to be received.

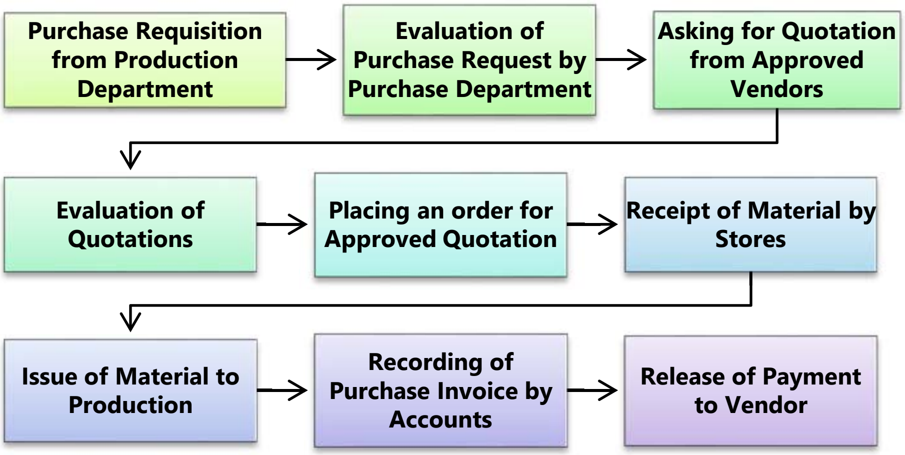

Purchase Requisition from Production Department
Evaluation of Purchase Request by Purchase Department
Asking for Quotation from Approved Vendors
Evaluation of Quotations
Placing an order for Approved Quotation
Receipt of Material by Stores
Issue of Material to Production
Recording of Purchase Invoice by Accounts
Release of Payment to Vendor

Fig. 2.6.6: Process showing Overall Purchase Process

- **Material Receipt:** This is a transaction of receipt of material against purchase order. This is commonly known as Material Receipt Note (MRN) or Goods Receipt Note (GRN). This transaction shall have a linking with Purchase Order. Information in Purchase Order is automatically copied to Material Receipt Voucher for saving time and efforts of user. Stock is increased after recording of this transaction.
- **Issue of Material:** Material received by stores shall be issued to production department as per requirement.
- **Purchase Invoice:** This is a financial transaction. Trial balance is affected due this transaction. Material Receipt transaction does not affect trial balance.

This transaction shall have a linking with Material Receipt Transaction and all the details of material received shall be copied automatically in purchase invoice. As stock is increased in Material Receipt transaction, it will not be increased again after recording of purchase invoice.

- **Payment to Vendor:** Payment shall be made to vendor based on purchase invoice recorded earlier. Payment transaction shall have a linking with purchase invoice.

Please note that Purchase Order and Material Receipt are not part of financial accounting and does not affect trial balance. But these transactions are part of overall Financial and Accounting System.

g. Quality Management Module

Quality Management (QM) Module helps in management of quality in productions across processes in an organization. This module helps an organization to accelerate their business by adopting a structured and functional way of managing quality in different processes. Quality Management module collaborates in procurement and sales, production, planning, inspection, notification, control, audit management and so on. Fig. 2.6.7 showing Process in Quality Management Module.

- ***Quality Planning:*** ***Quality planning is the process of planning the production activities to achieve the goals of meeting the customer requirements in time, within the available resources.***

- ***Quality Control:*** ***It is a system for ensuring the maintenance of proper standards in manufactured goods, especially by periodic random inspection of the product. IT involves the checking and monitoring of the process and products with an intention of preventing non-conforming materials from going to the customer. Various result areas are identified for each process and studies are conducted to verify whether those results are being achieved.***

- ***Quality Assurance:*** ***Quality assurance concentrates on identifying various processes, their interactions and sequence, defining the objectives of each process, identifying the key result areas and measures to measure the results, establishing the procedures for getting the required results, documenting the procedures to enable everyone to follow the same, educating the people to implement the procedures, preparing standard operating instructions to guide the people on work***

spot, monitoring and measuring the performance, taking suitable actions on deviations and continuously improving the systems.

- ***<u>Quality Improvement:</u> Quality improvement is a never-ending process. The customer's needs and expectations are continuously changing depending on the changes in technology, economy, political situation, ambitions and dreams, competition, etc.***

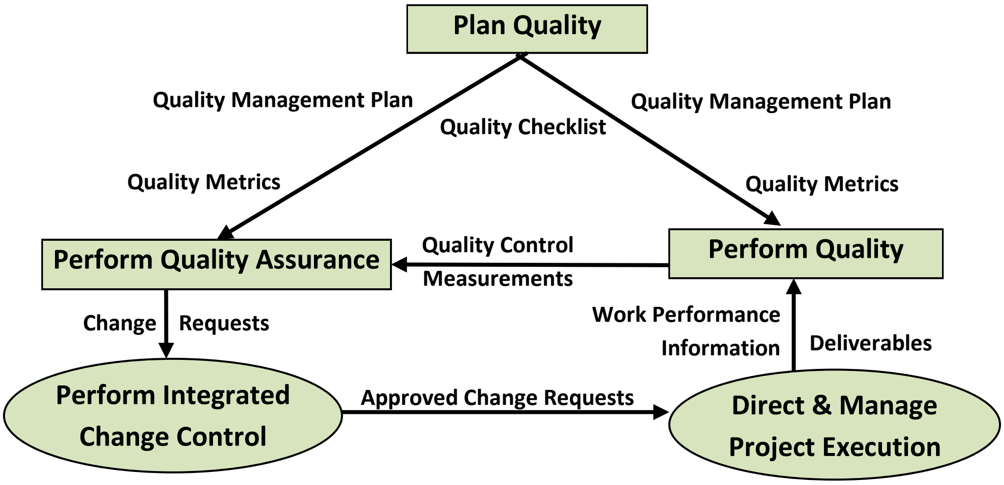


Fig. 2.6.7: Process in Quality Management Module

Quality Management Process includes the following:

- Master data and standards are set for quality management;
- Set Quality Targets to be met;
- Quality management plan is prepared;
- Define how those quality targets will be measured;
- Take the actions needed to measure quality;
- Identify quality issues and improvements and changes to be made;
- In case of any change is needed in the product, change requests are sent;
- Report on the overall level of quality achieved; and
- Quality is checked at multiple points, e.g. inwards of goods at warehouse, manufacturing, procurement, returns.

h. Plant Maintenance Module

Plant Maintenance (PM) is a functional module which handles the maintaining of equipment and enables efficient planning of production and generation schedules. This application component provides us a comprehensive software solution for all maintenance activities that are performed within a company. It supports cost-efficient maintenance methods such as risk-based maintenance or preventive maintenance, and provides comprehensive outage planning and powerful work order management.

Objectives of Plant Maintenance Module

(i) ***To achieve minimum breakdown and to keep the plant in good working condition at the lowest possible cost.***

(ii) ***To keep machines and other facilities in a condition that permits them to be used at their optimum (profit making) capacity without any interruption or hindrance.***

(iii) ***To ensure the availability of the machines, buildings and services required by other sections of the factory for the performance of their functions at optimum return on investment whether this investment be in material, machinery or personnel.***

Fig. 2.6.8 is showing process in Plant Maintenance.

- ***Equipment Master is a repository of the standard information that one needs related to a specific piece of equipment.***
- ***Equipment/Plant Maintenance provides a variety of reports to help us to review and manage information about our equipment and its maintenance.***
- ***Plant Maintenance (PM) Reports are used to review and manage information about preventive maintenance schedules and service types within any maintenance organization.***

Different PM reports are required to review PM information, such as:

- ***Status of service types for a piece of equipment;***
- ***Maintenance messages;***
- ***The frequency of occurrence for selected service types; and***
- ***All equipment transactions.***

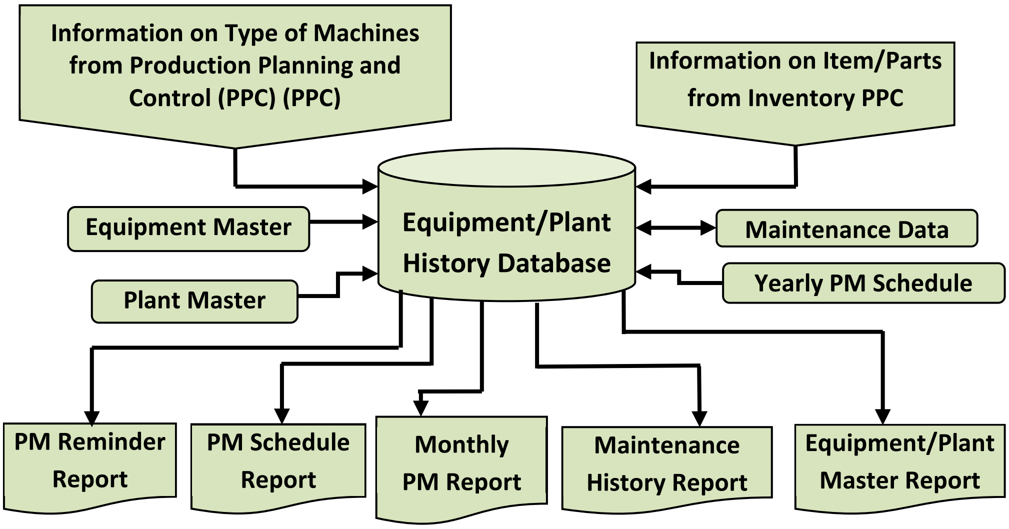

Information on Type of Machines from Production Planning and Control (PPC) (PPC)
Information on Item/Parts from Inventory PPC
Equipment Master
Plant Master
Equipment/Plant History Database
Maintenance Data
Yearly PM Schedule
PM Reminder Report
PM Schedule Report
Monthly PM Report
Maintenance History Report
Equipment/Plant Master Report

Fig. 2.6.8: Process in Plant Maintenance

i. Project Systems Module

This is an integrated project management tool used for planning and managing projects and portfolio management. It has several tools that enable project management process such as cost and planning budget, scheduling, requisitioning of materials and services, execution, until the project completion. Fig. 2.6.9 showing process in Project Systems.

Project System is closely integrated with other ERP modules like Logistics, Material Management, Sales and Distribution, Plant Maintenance, and Production Planning module etc. Before a project is initiated, it is required that project goal is clearly defined and the activities be structured. The Project Manager has a task to ensure that these projects are executed within budget and time and to ensure that resources are allocated to the project as per the requirement.

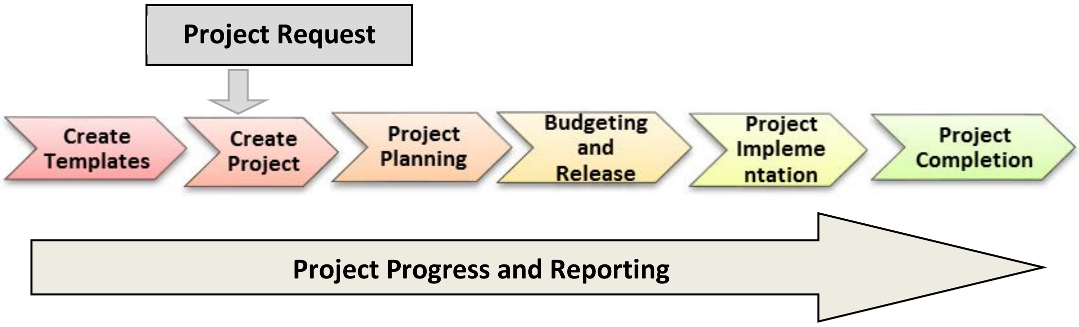


Fig. 2.6.9: Process in Project Systems

In Project System, each process has a defined set of tasks to be performed known as process flow in Project Lifecycle. When a project request is received, a project is created and it undergoes the following steps in project process flow / lifecycle.

j. Supply Chain Module

A Supply Chain is a network of autonomous or semi-autonomous business entities collectively responsible for procurement, manufacturing, and distribution activities associated with one or more families of related products. This module provides extensive functionality for logistics, manufacturing, planning, and analytics. In other words, a supply chain is a network of facilities that procure raw materials, transform them into intermediate goods and then finished products, and then finally deliver the products to customers through a distribution system or a chain.

You can optimize your supply chain for months in advance; streamline processes such as supply network, demand, and material requirement planning; create detailed scheduling; refine production integration, and maximize transportation scheduling. Fig. 2.6.10 showing process in supply chain.

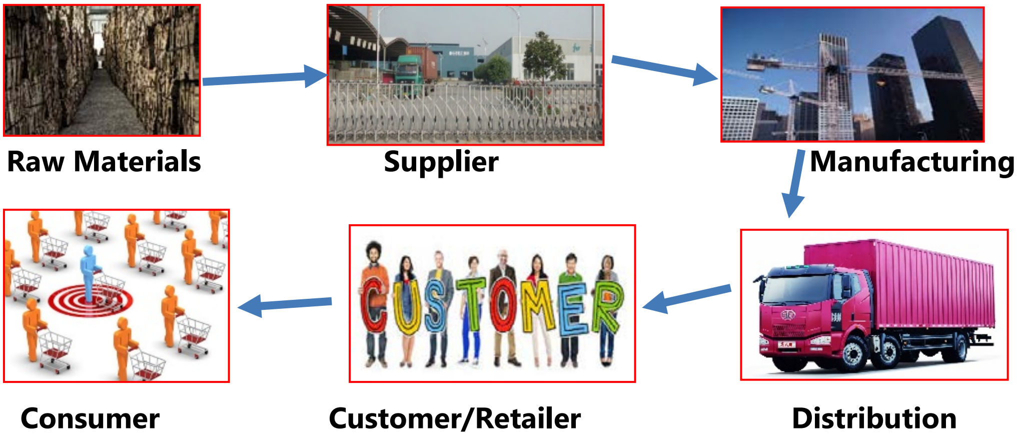


Fig. 2.6.10: Process in Supply Chain

In Supply Chain Management System, any product which is manufactured in a company, first reaches directly from manufacturer to distributors where manufacturer sells the product to the distributor with some profit of margin. Distributors supply that product to retailer with his/her profit and then finally customers receive that product from retailer. This is called <u>Supply Chain</u>

Management System ***which implies that a product reaches from manufacturer to customer through supply.***

k. Customer Relationship Management (CRM)

Customer Relationship Management is a system which aims at improving the relationship with existing customers, finding new prospective customers, and winning back former customers. This system can be brought into effect with software which helps in collecting, organizing, and managing the customer information.

CRM manages the enterprise's relationship with its customers. This includes determining who the high-value customers are and documenting what interactions the customers have had with the enterprise. Only large ERP packages have a CRM module. The CRM module uses the existing ERP tables as the source of its data. This is primarily the Contact, Customer, and Sales tables. CRM does not exchange transactions with other modules as CRM does not have transactions. Implementing a CRM strategy is advantageous to both small-scale and large-scale business ventures. Key benefits of a CRM module are as under.

- **Improved customer relations:** One of the prime benefits of using a CRM is obtaining better customer satisfaction. By using this strategy, all dealings involving servicing, marketing, and selling out products to the customers can be carried out in an organized and systematic way. Better services can be provided to customers through improved understanding of their issues and this in turn helps in increasing customer loyalty and decreasing customer agitation. In this way, continuous feedback from the customers regarding the products and services can be received. It is also possible that the customers may recommend the product to their acquaintances, when efficient and satisfactory services are provided.
- **Increase customer revenues:** By using a CRM strategy for any business, the revenue of the company can be increased. Using the data collected, marketing campaigns can be popularized in a more effective way. With the help of CRM software, it can be ensured that the product promotions reach a different and brand new set of customers, and not the ones who had already purchased the product, and thus effectively increase the customer revenue.
- **Maximize up-selling and cross-selling:** A CRM system allows up-selling which is the practice of giving customers premium products that fall in the same category of their purchase. The strategy also facilitates cross selling which is the practice of offering complementary products to customers, based on their

previous purchases. This is done by interacting with the customers and getting an idea about their wants, needs, and patterns of purchase. The details thus obtained will be stored in a central database, which is accessible to all company executives. So, when an opportunity is spotted, the executives can promote their products to the customers, thus maximizing up-selling and cross selling.

- **Better internal communication:** Following a CRM strategy helps in building up better communication within the company. The sharing of customer data between different departments will enable them to work as a team. This is better than functioning as an isolated entity, as it will help in increasing the company's profitability and enabling better service to customers.
- **Optimize marketing:** CRM enables to understand the customer needs and behavior in a better way, thereby allowing any enterprise to identify the correct time to market its product to the customers. CRM will also give an idea about the most profitable customer groups, and by using this information, similar prospective groups, at the right time will be targeted. In this way, marketing resources can be optimized efficiently and time is not wasted on less profitable customer groups.

2.6.4 Integration with Other Modules

Any ERP System is like human body. There are different units and each unit relates to another units. All the units must work in harmony with other units to generate desired result. Following points are important for integration of modules with Financial and Accounting System:

- Master data across all the modules must be same and must be shared with other modules where-ever required.
- Common transaction data must be shared with other modules where-ever required.
- Separate voucher types to be used for each module for easy identification of department recording it.
- Figures and transaction may flow across the department, e.g. closing stock value is taken to Trading Account as well as Balance Sheet. Correct closing stock value is dependent on two things, complete and correct accounting of inventory transactions and appropriate method of valuation of closing stock. Closing stock quantity is required by Purchase Department, Stores Department, Accounts Department, and Production Department, Similarly, salary figures are used by Human Resource Department and Accounts

Department simultaneously. Hence, it is necessary to design the system accordingly.

I. Integration Points

Some of the points regarding integration with other modules are discussed here.

(i) Material Management Integration with Finance and Controlling (FICO)

It is integrated in the area like Material Valuation, Vendor payments, Material costing etc. Whenever any inventory posting is done, it updates the General Ledger (G/L) accounts online in the background. Logistics invoice verification will create vendor liability in vendor account immediately on posting the document. Any advance given against the purchase order updates the Purchase Order history. For every inventory posting, there is corresponding Controlling document to update profit centre accounting reporting.

(ii) Human Resource Module Integration with Finance and Controlling

Attendance and leave record is used for calculation of salary on monthly basis. Salary is also a part of financial accounting. Hence salary processed and calculated by Human Resource Module shall be integrated with Finance & Controlling Module.

(iii) Material Management Integration with Production Planning (PP)

It is integrated in the areas like Material Requirement Planning, Receipts/issues against production orders, Availability check for stocks etc. Material requirement Planning is d- based on Stocks, expected receipts, expected issues. It generates planned orders or purchase requisitions which can be converted to purchase orders/Contracts. Inventory Management is responsible for staging of the components required for production orders. The receipt of the finished products in the Warehouse is posted in Inventory Management.

(iv) Material Management Integration with Sales and Distribution (SD)

It is integrated in the areas like Delivery, Availability Check, Stock transfers requirements etc. As soon as a sales order is created, it can initiate a dynamic availability check of stocks on hand. When the delivery is created, the quantity to be delivered is marked as "Scheduled for delivery". It is deducted from the total stock when the goods issue is posted. Purchase order can be directly converted to delivery for a stock transfer requirement.

(v) Material Management Integration with Quality Management (QM)

It is integrated with QM for Quality inspection at Goods Receipt, In process inspection etc. In the case of a goods movement, the system determines whether the material is subject to an inspection operation. If so, a corresponding activity is initiated for the movement in the Quality Management system. Based on quality parameters vendor evaluation is done.

(vi) Material Management Integration with Plant Maintenance (PM)

The material/service requirement is mentioned in Maintenance order. This leads to generation of Purchase Requisition. This PR will be converted to Purchase Order by MM. The goods for a PO will be in warded to Maintenance by MM. The spares which were reserved for maintenance order will be issued by MM against the reservation number.

II. Example of ERP Modules

Let us consider a case of an ice-cream manufacturing company.

A. Material Management Module

a. Placing a purchase order for purchase of raw material like milk, dry fruits, milk powder, butter, essence, sugar, etc. on an approved vendor.

b. Received raw material at stores.

B. Production Module

a. Seeking raw material from stores.

b. Converting raw material into WIP and WIP into finished goods.

c. Sending the finished goods to cold room.

C. Supply Chain Module

a. Distributing finished goods, i.e. ice cream to the customers.

b. Keeping a track of all deliveries.

c. Planning and scheduling of all deliveries.

D. Finance & Accounting

a. Recording of all financial transactions.

b. Payments to vendors.

c. Collections from customers.

E. Human Resource Module

a. Keeping record of all human resource related activities.

b. Attendance, leave, salary calculations, joining and leaving of employees.

F. Sales & Distribution

a. Performing pre-sales activities.

b. Recording sales orders.

c. Keeping track of all customer related transactions till collection against invoices.

2.7 REPORTING SYSTEM AND MANAGEMENT INFORMATION SYSTEMS (MIS)

2.7.1 Reporting System

A **Report** simply means presentation of information in proper and meaningful way. We have already discussed about system earlier. So, basically reporting system is a system of regular reporting on the pre-decided aspects.

The basic purpose of any Financial and Accounting system is to give right information at right point of time to right people for right decision making. Two basic reports, i.e. **Balance Sheet** and **Profit & Loss Account** are used for basic analysis of financial position and financial performance. But only these two reports are not sufficient for all types of decision making. Hence, we need a proper reporting system to serve the purpose.

Companies generally have a finance function which monitors the financial position monthly. Key reports are analysed by management to determine if appropriate financial decisions are made at the right time. For example, comparing actual revenue by region and comparing to budgets to ensure forecasts are met. These periodic reviews also ensure financial hygiene is kept and no mis-statements creep in, in the preparation of year-end financial reports.

Companies especially the large listed corporations publish their annual reports to public at large providing many insights as to their operations, their future and their social responsibilities too. MD&A (Management Discussion & Analysis) section in these annual reports discusses how management have prepared the financial position, their interpretation of the company's performance, the industry in which they operate and provide critical guidance on where the company is heading.

2.7.2 Management Information System (MIS)

An **MIS** report is a tool that managers use to evaluate business processes and operations. There are different kinds of MIS reports and that may be used to visually present different kinds of information.

I. What is an MIS Report?

Assume that you are the manager of a medium-sized company's customer service department. Your staff takes phone calls and emails from over 300 customers every day. For the most part, they do a very good job, but recently, customers have started to complain that it takes too long to get their questions answered. Upper management at your company is concerned about this and wants to know what they can do to fix the problem. But before they decide, they need you to give them more information. How will you do this?

This is where MIS reports come in. Business managers at all levels of an organization, from assistant managers to executives, rely on reports generated from these systems to help them evaluate their business' daily activities or problems that arise, make decisions, and track progress. MIS system reporting is used by businesses of all sizes and in every industry.

II. Who Uses MIS Reports?

MIS systems automatically collect data from various areas within a business. These systems can produce daily reports that can be sent to key members throughout the organization. Most MIS systems can also generate on-demand reports. On-demand MIS reports allow managers and other users of the system to generate an MIS report whenever they need it. Many large businesses have specialized MIS departments, whose only job is to gather business information and create MIS reports. Some of these businesses use sophisticated computing technology and software to gather information. However, the method of collecting information does not have to be that complex. Smaller businesses often use simple software programs and spreadsheets for their MIS reporting needs.

There can be as many types of MIS reports as there are divisions within a business. For example, information about sales revenue and business expenses would be useful in MIS reports for finance and accounting managers. Warehouse managers would benefit from MIS reports about product inventory and shipping information. Total sales from the past year could go into an MIS report for marketing and sales managers.

III. Type of Information in a MIS Report

In our pretend manager example, you've been asked to present information about your department's customer service calls. An MIS report for this would likely contain data such as:

- ♦ The number of calls your staff takes;

- The number of emails that come in each day;
- The average amount of time it takes to answer a phone call or email; and
- The number of questions that your staff answers correctly vs. the number that are incorrect.

To make this information most useful, you also need to ensure that it meets the following criteria:

- **Relevant -** MIS reports need to be specific to the business area they address. This is important because a report that includes unnecessary information might be ignored.
- **Timely -** Managers need to know what's happening now or in the recent past to make decisions about the future. Be careful not to include information that is old. An example of timely information for your report might be customer phone calls and emails going back 12 months from the current date.
- **Accurate -** It's critical that numbers add up and that dates and times are correct. Managers and others who rely on MIS reports can't make sound decisions with information that is wrong. Financial information is often required to be accurate to the dollar. In other cases, it may be OK to round off numbers.
- **Structured -** Information in an MIS report can be complicated. Making that information easy to follow helps management understand what the report is saying. Try to break long passages of information into more readable blocks or chunks and give these chunks meaningful headings.

IV. Example of MIS Report

Let us take a case of MIS Report regarding control over cash balance. The objective of this MIS report is to have control over cash balance and accounting of cash transactions.

A simple report of weekly cash report is depicted in the Table 2.7.1.

Table 2.7.1: Image of weekly cash report

Indradhanu Consulting Private Limited						
Weekly Cash Report						
Date	Physical Cash				System Cash	Difference
	Opening Balance	Total Receipts	Total Payments	Closing Balance		
1/7/2017	40,200	13,043	15,403	37,840	37,840	-

2/7/2017	37,840	45,760	33,443	50,157	50,157	-
3/7/2017	50,157	45,300	23,009	72,448	72,448	-
4/7/2017	72,448	32,333	34,200	70,581	70,581	-
5/7/2017	70,581	7,600	8,131	70,050	70,100	50
6/7/2017	70,050	56,400	17,050	109,400	109,400	-
7/7/2017	109,400	60,000	30,100	139,300	139,300	-

This report can be further improved by adding date wise denomination of notes as shown under in the Table 2.7.2.

Table 2.7.2: Improved version of Sales MIS Report of weekly cash

Denominations	2000	500	100	50	20	10	5	2	1	Coins	Total
1/7/2017											
Quantity	10	20	25	60	60	111	2	5	10	0	
Value	20,000	10,000	2,500	3,000	1,200	1,110	10	10	10	-	37,840

For a sales' oriented business, Sales MIS Report can be designed as under in Table 2.7.3.

Table 2.7.3: Sales MIS Report

Month	Demos Shown	Sales		
		No.	Value	Collection
Apr-17	38	12	148,800	129,600
May-17	42	13	161,200	140,400
Jun-17	33	15	186,000	162,000
Jul-17	45	21	260,400	226,800
Aug-17	50	22	272,800	237,600
Sep-17	26	14	173,600	151,200
Oct-17	29	10	124,000	108,000
Nov-17	44	28	347,200	347,200
Dec-17	32	21	260,400	226,800
Jan-18	43	16	198,400	172,800
Feb-18	53	27	334,800	291,600
Mar-18	47	20	248,000	216,000
Total	**482**	**219**	**2,715,600**	**2,410,000**
Unattended Prospects				48

2.8 DATA ANALYTICS AND BUSINESS INTELLIGENCE

Data Analytics is the process of examining data sets to draw conclusions about the information they contain, increasingly with the aid of specialized systems and software. Data analytics technologies and techniques are widely used in commercial industries to enable organizations to make more-informed business decisions and by scientists and researchers to verify or disprove scientific models, theories and hypotheses.

As a term, Data Analytics predominantly refers to an assortment of applications, from basic Business Intelligence (BI), reporting and Online Analytical Processing (OLAP) to various forms of advanced analytics. In that sense, it's similar in nature to business analytics, another umbrella term for approaches to analysing data - with the difference that the latter is oriented to business uses, while data analytics has a broader focus. The expansive view of the term isn't universal, though: In some cases, people use data analytics specifically to mean advanced analytics, treating Business Intelligence (BI) as a separate category.

Data Analytics initiatives can help businesses increase revenues, improve operational efficiency, optimize marketing campaigns and customer service efforts, respond more quickly to emerging market trends and gain a competitive edge over rivals -- all with the goal of boosting business performance. Depending on the particular application, the data that's analysed can consist of either historical records or new information that has been processed for real-time analytics uses. In addition, it can come from a mix of internal systems and external data sources.

2.8.1 Types of Data Analytics Applications

At a high level, Data Analytics methodologies include **Exploratory Data Analysis (EDA)**, which aims to find patterns and relationships in data, and **Confirmatory Data Analysis (CDA)**, which applies statistical techniques to determine whether hypotheses about a data set are True or False. EDA is often compared to detective work, while CDA is akin to the work of a judge or jury during a court trial - a distinction first drawn by statistician John W. Tukey in his 1977 book Exploratory Data Analysis. Data Analytics can also be separated into **Quantitative Data Analysis** and **Qualitative Data Analysis.**

- **Quantitative Data Analysis:** This involves analysis of numerical data with quantifiable variables that can be compared or measured statistically.

- **Qualitative Data Analysis:** The qualitative approach is more interpretive - it focuses on understanding the content of non-numerical data like text, images, audio and video, including common phrases, themes and points of view.

At the application level, Business Intelligence and reporting provides business executives and other corporate workers with actionable information about key performance indicators, business operations, customers and more. In the past, Data queries and reports typically were created for end users by BI developers working in IT or for a centralized BI team; now, organizations increasingly use self-service BI tools that let executives, business analysts and operational workers run their own ad hoc queries and build reports themselves. More advanced types of Data Analytics include–

- **Data Mining**, which involves sorting through large data sets to identify trends, patterns and relationships;
- **Predictive Analytics**, which seeks to predict customer behaviour, equipment failures and other future events; and
- **Machine Learning**, an artificial intelligence technique that uses automated algorithms to churn through data sets more quickly than data scientists can do via conventional analytical modelling.

Big Data Analytics applies data mining, predictive analytics and machine learning tools to sets of big data that often contain unstructured and semi-structured data. Text mining provides a means of analysing documents, emails and other text-based content. Fig. 2.8.1 showing the process of converting raw data into knowledge.

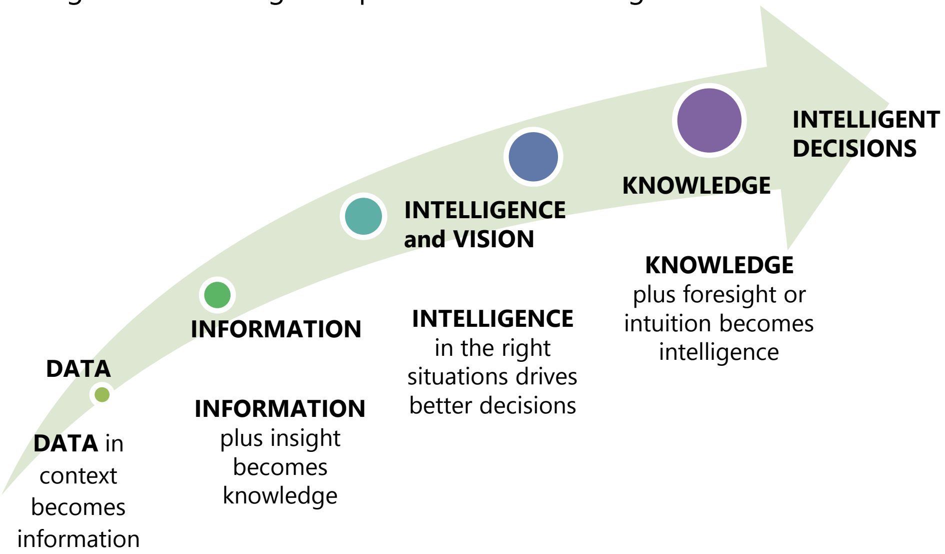

INTELLIGENT DECISIONS
KNOWLEDGE
INTELLIGENCE and VISION
INFORMATION
DATA
KNOWLEDGE plus foresight or intuition becomes intelligence
INTELLIGENCE in the right situations drives better decisions
INFORMATION plus insight becomes knowledge
DATA in context becomes information

Fig. 2.8.1: Process of converting raw data into knowledge

Some Application areas of Data Analytics are as follows:

- Data Analytics initiatives support a wide variety of business uses. For example, banks and credit card companies analyse withdrawal and spending patterns to prevent fraud and identity theft.
- E-commerce companies and marketing services providers do clickstream analysis to identify website visitors who are more likely to buy a product or service based on navigation and page-viewing patterns.
- Mobile network operators examine customer data to forecast so they can take steps to prevent defections to business rivals; to boost customer relationship management efforts. Other companies also engage in CRM analytics to segment customers for marketing campaigns and equip call centre workers with up-to-date information about callers.
- Healthcare organizations mine patient data to evaluate the effectiveness of treatments for cancer and other diseases.

2.8.2 Inside the Data Analytics Process

Data Analytics applications involve more than just analysing data. Particularly on advanced analytics projects, much of the required work takes place upfront, in collecting, integrating and preparing data and then developing, testing and revising analytical models to ensure that they produce accurate results. In addition to data scientists and other data analysts, analytics teams often include data engineers, whose job is to help get data sets ready for analysis.

The analytics process starts with data collection, in which data scientists identify the information they need for an analytics application and then work on their own or with data engineers and IT staffers to assemble it for use. Data from different source systems may need to be combined via data integration routines transformed into a common format and loaded into an analytics system, such as a Hadoop cluster, NoSQL database or data warehouse. In other cases, the collection process may consist of pulling a relevant subset out of a stream of raw data that flows into, say, Hadoop and moving it to a separate partition in the system so it can be analysed without affecting the overall data set.

Once the data that's needed is in place, the next step is to find and fix data quality problems that could affect the accuracy of analytics applications. That includes running data profiling and data cleansing jobs to make sure that the information in a data set is consistent and that errors and duplicate entries are eliminated. Additional data preparation work is then done to manipulate and organize the data for the planned analytics use, and data governance policies are applied to ensure that the data hews to corporate standards and is being used properly.

At that point, the data analytics work begins in earnest. A data scientist builds an analytical model, using predictive modelling tools or other analytics software and programming languages such as Python, Scala, R and SQL. The model is initially run against a partial data set to test its accuracy; typically, it's then revised and tested again, a process known as "training" the model that continues until it functions as intended. Finally, the model is run in production mode against the full data set, something that can be done once to address a specific information need or on an ongoing basis as the data is updated.

In some cases, analytics applications can be set to automatically trigger business actions -- for example, stock trades by a financial services firm. Otherwise, the last step in the data analytics process is communicating the results generated by analytical models to business executives and other end users to aid in their decision-making. That usually is done with the help of data visualization techniques, which analytics teams use to create charts and other infographics designed to make their findings easier to understand. Data visualizations often are incorporated into BI dashboard applications that display data on a single screen and can be updated in real time as new information becomes available.

2.8.3 Business Intelligence (BI)

Business Intelligence (BI) is a technology-driven process for analysing data and presenting actionable information to help corporate executives, business managers and other end users make more informed business decisions. BI encompasses a wide variety of tools, applications and methodologies that enable organizations to collect data from internal systems and external sources, prepare it for analysis, develop and run queries against the data, and create reports, dashboards and data visualizations to make the analytical results available to corporate decision makers as well as operational workers.

Reasons for Business Intelligence

BI enables organizations to make well-informed business decisions and thus can be the source of competitive advantages. This is especially true when we can extrapolate information from indicators in the external environment and make accurate forecasts about future trends or economic conditions. Once business intelligence is gathered effectively and used proactively, we can make decisions that benefit our organization before the competition does.

The ultimate objective of business intelligence is to improve the timeliness and quality of information. Business intelligence reveals to us –

- ***The position of the firm in comparison to its competitors***
- ***Changes in customer behaviour and spending patterns***
- ***The capabilities of the firm***
- ***Market conditions future trends, demographic and economic information***
- ***The social, regulatory and political environment***
- ***What the other firms in the market are doing***

Fig. 2.8.2 showing example of Business Intelligence use. Business Intelligence uses data from different sources and helps to finds answers to various questions as shown on right hand side of the Fig.

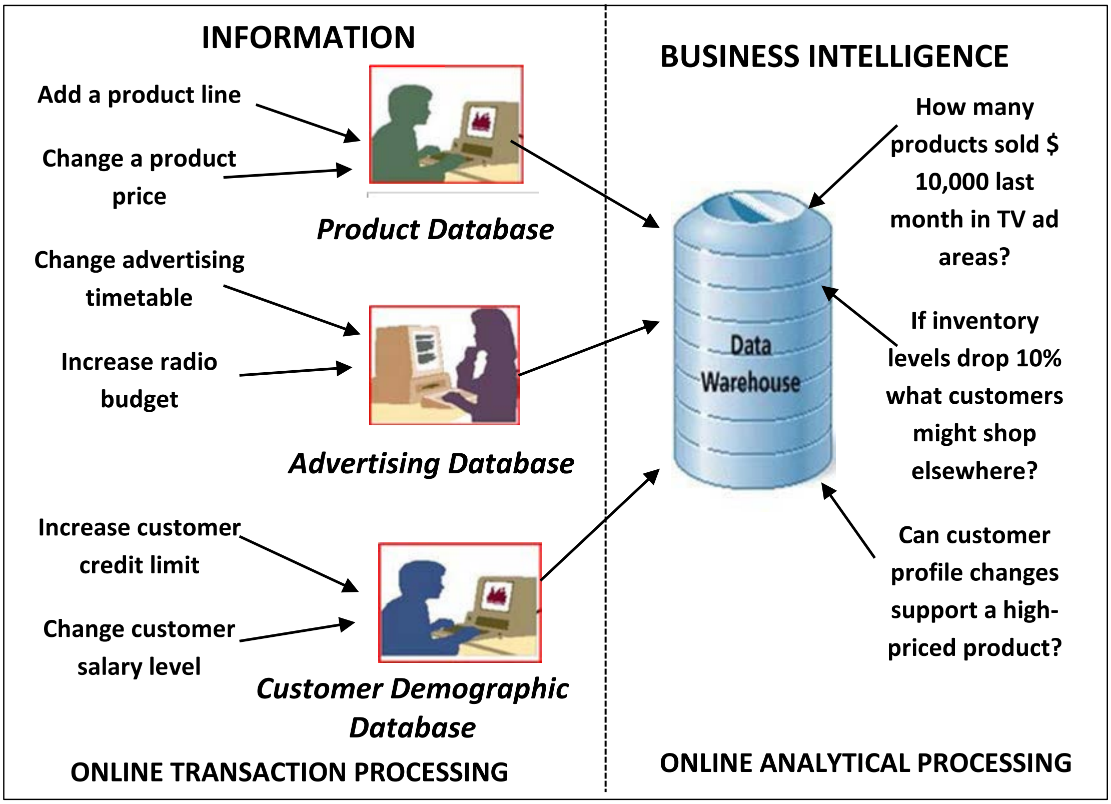

INFORMATION
Add a product line
Change a product price
Product Database
Change advertising timetable
Increase radio budget
Advertising Database
Increase customer credit limit
Change customer salary level
Customer Demographic Database
ONLINE TRANSACTION PROCESSING
BUSINESS INTELLIGENCE
Data Warehouse
How many products sold $ 10,000 last month in TV ad areas?
If inventory levels drop 10% what customers might shop elsewhere?
Can customer profile changes support a high-priced product?
ONLINE ANALYTICAL PROCESSING

Fig. 2.8.2: Example of Business Intelligence

BI data can include historical information, as well as new data gathered from source systems as it is generated, enabling BI analysis to support both strategic and tactical decision-making processes. Initially, BI tools were primarily used by data analysts and other IT professionals who ran analyses and produced reports with query results for business users. Increasingly, however, business executives and workers are using BI software themselves, thanks partly to the development of self-service BI and data discovery tools.

Benefits of Business Intelligence

♦ BI improves the overall performance of the company using it. The potential benefits of business intelligence programs include –

  o accelerating and improving decision making;

  o optimizing internal business processes;

  o enhancing communication among departments while coordinating activities;

  o increasing operational efficiency;

  o driving new revenues; and

  o gaining competitive advantages over business rivals.

♦ BI systems can also help companies identify market trends and spot business problems that need to be addressed.

♦ BI systems help in enhancing customer experience, allowing for the timely and appropriate response to customer problems and priorities.

Business Intelligence Technology

Business Intelligence combines a broad set of data analysis applications, including ad hoc analysis and querying, enterprise reporting, Online Analytical Processing (OLAP), mobile BI, real-time BI, operational BI, cloud and software as a service BI, open source BI, collaborative BI and location intelligence.

BI technology also includes data visualization software for designing charts and other info-graphics, as well as tools for building BI dashboards and performance scorecards that display visualized data on business metrics and key performance indicators in an easy-to-grasp way. BI applications can be bought separately from different vendors or as part of a unified BI platform from a single vendor.

BI programs can also incorporate forms of advanced analytics, such as data mining, predictive analytics, text mining, statistical analysis and big data analytics. In many cases, though, advanced analytics projects are conducted and managed by separate teams of data scientists, statisticians, predictive modellers and other skilled analytics professionals, while BI teams oversee more straightforward querying and analysis of business data.

Business Intelligence data typically is stored in a data warehouse or smaller data marts that hold subsets of a company's information. In addition, Hadoop systems are increasingly being used within BI architectures as repositories or landing pads for BI and analytics data, especially for unstructured data, log files, sensor data and other types of big data. Before it's used in BI applications, raw data from different source systems must be integrated, consolidated and cleansed using data integration and data quality tools to ensure that users are analysing accurate and consistent information.

In addition to BI managers, Business Intelligence teams generally include a mix of BI architects, BI developers, business analysts and data management professionals; business users often are also included to represent the business side and make sure its needs are met in the BI development process. To help with that, a growing number of organizations are replacing traditional waterfall development with Agile BI and data warehousing approaches that use Agile software development techniques to break up BI projects into small chunks and deliver new functionality to end users on an incremental and iterative basis. Doing so can enable companies to put BI features into use more quickly and to refine or modify development plans as business needs change or new requirements emerge and take priority over earlier ones.

Business intelligence is sometimes used interchangeably with business analytics; in other cases, business analytics is used either more narrowly to refer to advanced data analytics or more broadly to include both BI and advanced analytics.

2.9 BUSINESS REPORTING AND FUNDAMENTALS OF XBRL

2.9.1 Business Reporting

Business Reporting or **Enterprise Reporting** is the public reporting of operating and financial data by a business enterprise or the regular provision of information to decision-makers within an organization to support them in their work.

Reporting is a fundamental part of the larger movement towards improved business intelligence and knowledge management. Often implementation involves Extract, Transform, and Load (ETL) procedures in coordination with a data warehouse and then using one or more reporting tools. While reports can be distributed in print form or via email, they are typically accessed via a corporate intranet.

With the dramatic expansion of information technology, and the desire for increased competitiveness in corporations, there has been an increase in the use of computing power to produce unified reports which join different views of the enterprise in one place. This reporting process involves querying data sources with different logical models to produce a human readable report - for example; a computer user has to query the Human Resources databases and the Capital Improvements databases to show how efficiently space is being used across an entire corporation.

Organizations conduct a wide range of reporting, including financial and regulatory reporting; Environmental, Social, and Governance (ESG) reporting (or sustainability reporting); and, increasingly, integrated reporting.

Organizations communicate with their stakeholders about:

- mission, vision, objectives, and strategy;
- governance arrangements and risk management;
- trade-offs between the shorter- and longer-term strategies; and
- financial, social, and environmental performance (how they have fared against their objectives in practice).

Why is Business Reporting Important?

Effective and transparent business reporting allows organizations to present a cohesive explanation of their business and helps them engage with internal and external stakeholders, including customers, employees, shareholders, creditors, and regulators.

High-quality business reporting is at the heart of strong and sustainable organizations, financial markets, and economies, as this information is crucial for stakeholders to assess organizational performance and make informed decisions with respect to an organization's capacity to create and preserve value. (Value in this context is not necessarily limited to monetary value, but can also comprise, for example, social, environmental, or wider economic value.) As organizations fully depend on their stakeholders for sustainable success, it is in their interest to provide them with high-quality reports. For example, effective high-quality reporting reduces the risk for lenders and may lower the cost of capital.

Many organizations are increasingly complex, and have larger economic, environmental, and social footprints. Thus, various stakeholder groups are demanding increased Environmental, Social and Global (ESG) information, as well as greater insight into how these factors affect financial performance and valuations.

High-quality reports also promote better internal decision-making. High-quality information is integral to the successful management of the business, and is one of the major drivers of sustainable organizational success.

2.9.2 Fundamentals of XBRL

XBRL (eXtensible Business Reporting Language) is a freely available and global standard for exchanging business information. XBRL allows the expression of semantic meaning commonly required in business reporting. The language is XML-based and uses the XML syntax and related XML technologies such as XML Schema, XLink, XPath, and Namespaces. One use of XBRL is to define and exchange financial information, such as a financial statement. The XBRL Specification is developed and published by XBRL International, Inc. (XII).

I. What is XBRL?

XBRL is the open international standard for digital business reporting, managed by a global not for profit consortium, XBRL International. XBRL is used around the world, in more than 50 countries. Millions of XBRL documents are created every year, replacing older, paper-based reports with more useful, more effective and more accurate digital versions.

In a nutshell, XBRL provides a language in which reporting terms can be authoritatively defined. Those terms can then be used to uniquely represent the contents of financial statements or other kinds of compliance, performance and business reports. XBRL let's reporting information move between organizations rapidly, accurately and digitally.

XBRL is a standards-based way to communicate and exchange business information between business systems. These communications are defined by metadata set out in taxonomies, which capture the definition of individual reporting concepts as well as the relationships between concepts and other semantic meaning. Information being communicated or exchanged is provided within an XBRL instance.

The change from paper, PDF and HTML based reports to XBRL ones is a little bit like the change from film photography to digital photography, or from paper maps to digital maps. The new format allows you to do all the things that used to be possible, but also opens up a range of new capabilities because the information is clearly defined, platform-independent, testable and digital. Just like digital maps, digital business reports, in XBRL format, simplify the way that people can use, share, analyse and add value to the data.

II. What does XBRL do?

Often termed "bar codes for reporting", XBRL makes reporting more accurate and more efficient. It allows unique tags to be associated with reported facts, allowing:

- people publishing reports to do so with confidence that the information contained in them can be consumed and analysed accurately.
- people consuming reports to test them against a set of business and logical rules, to capture and avoid mistakes at their source.
- people using the information to do so in the way that best suits their needs, including by using different languages, alternative currencies and in their preferred style.
- people consuming the information to do so confident that the data provided to them conforms to a set of sophisticated pre-defined definitions.

III. What is XBRL tagging?

XBRL Tagging is the process by which any financial data is tagged with the most appropriate element in an accounting taxonomy (a dictionary of accounting terms) that best represents the data in addition to tags that facilitate identification/classification (such as enterprise, reporting period, reporting currency, unit of measurement etc.). Since all XBRL reports use the same taxonomy, numbers associated with the same element are comparable irrespective of how they are described by those releasing the financial statements.

Comprehensive definitions and accurate data tags allow preparation, validation, publication, exchange, consumption; and analysis of business information of all kinds. Information in reports prepared using the XBRL standard is interchangeable between different information systems in entirely different organizations. This allows for the exchange of business information across a reporting chain. People that want to report information, share information, publish performance information and allow straight through information processing all rely on XBRL.

In addition to allowing the exchange of summary business reports, like financial statements, and risk and performance reports, XBRL has the capability to allow the tagging of transactions that can themselves be aggregated into XBRL reports. These transactional capabilities allow system-independent exchange and analysis of significant quantities of supporting data and can be the key to transforming reporting supply chains.

IV. Who uses it?

The international XBRL consortium is supported by more than 600 member organizations, from both the private and public sectors. The standard has been developed and refined over more than a decade and supports almost every kind of conceivable reporting, while providing a wide range of features that enhance the quality and consistency of reports, as well as their usability. XBRL is used in many ways, for many different purposes, including by:

(i) Regulators

- Financial regulators that need significant amounts of complex performance and risk information about the institutions that they regulate.
- Securities regulators and stock exchanges that need to analyse the performance and compliance of listed companies and securities, and need to ensure that this information is available to markets to consume and analyse.
- Business registrars that need to receive and make publicly available a range of corporate data about private and public companies, including annual financial statements.
- Tax authorities that need financial statements and other compliance information from companies to process and review their corporate tax affairs.
- Statistical and monetary policy authorities that need financial performance information from many different organizations.

(ii) Companies

- Companies that need to provide information to one or more of the regulators mentioned above.
- Enterprises that need to accurately move information around within a complex group.
- Supply chains that need to exchange information to help manage risk and measure activity.

(iii) Governments

- Government agencies that are simplifying the process of businesses reporting to government and reducing red tape, by either harmonizing data definitions or consolidating reporting obligations (or both).
- Government agencies that are improving government reporting by standardizing the way that consolidated or transactional reports are prepared and used within government agencies and/or published into the public domain.

(iv) Data Providers

- Specialist data providers that use performance and risk information published into the market place and create comparisons, ratings and other value-added information products for other market participants.

(v) Analysts and Investors

- Analysts that need to understand relative risk and performance.
- Investors that need to compare potential investments and understand the underlying performance of existing investments.

(vi) Accountants

- Accountants use XBRL in support of clients reporting requirements and are often involved in the preparation of XBRL reports.

V. Important features of XBRL

♦ **Clear Definitions:** XBRL allows the creation of reusable, authoritative definitions, called taxonomies that capture the meaning contained in all the reporting terms used in a business report, as well as the relationships between all the terms. Taxonomies are developed by regulators, accounting standards setters, government agencies and other groups that need to clearly define information that needs to be reported upon. XBRL doesn't limit what kind of information is defined: it's a language that can be used and extended as needed.

♦ **Testable Business Rules:** XBRL allows the creation of business rules that constrain what can be reported. Business rules can be logical or mathematical, or both and can be used, for example, these business rules can be used to:

- stop poor quality information being sent to a regulator or third party, by being run by the preparer while the report is in draft.

  - stop poor quality information being accepted by a regulator or third party, by being run at the point that the information is being received. Business reports that fail critical rules can be bounced back to the preparer for review and resubmission.
  - flagging or highlighting questionable information, allowing prompt follow up, correction or explanation.
  - create ratios, aggregations and other kinds of value-added information, based on the fundamental data provided.

- **Multi-lingual Support:** XBRL allows concept definitions to be prepared in as many languages as necessary. Translations of definitions can also be added by third parties. This means that it's possible to display a range of reports in a different language to the one that they were prepared in, without any additional work. The XBRL community makes extensive use of this capability as it can automatically open up reports to different communities.
- **Strong Software Support:** XBRL is supported by a very wide range of software from vendors large and small, allowing a very wide range of stakeholders to work with the standard.

2.10 APPLICABLE REGULATORY & COMPLIANCE REQUIREMENTS

2.10.1 What is Regulatory Compliance?

In general, **Compliance** means conforming to a rule, such as a specification, policy, standard or law. **Regulatory Compliance** describes the goal that organizations aspire to achieve in their efforts to ensure that they are aware of and take steps to comply with relevant laws, policies, and regulations. Due to the increasing number of regulations and need for operational transparency, organizations are increasingly adopting the use of consolidated and harmonized sets of compliance controls. This approach is used to ensure that all necessary governance requirements can be met without the unnecessary duplication of effort and activity from resources.

Regulatory compliance is an organization's adherence to laws, regulations, guidelines and specifications relevant to its business. Violations of regulatory compliance regulations often result in legal punishment, including interest, penalty and prosecution in some cases.

By and large we can classify the compliance and regulatory requirements in two types as under.

a. **General –** Applicable to all irrespective of anything.

b. **Specific –** Applicable to specific type of businesses only.

E.g. Income Tax compliance is applicable to all subject to basic exemption limit. But compliance regarding GST, Labour Law, Company Law, etc. are applicable to specific type of businesses / entities only.

2.10.2 Regulatory Compliance and Accounting Systems

Regulatory compliance and accounting systems are closely connected with each other. Most of the regulatory compliance requires accounting data and accounting data comes from accounting systems. E.g. Income tax returns are prepared based on accounting data only. There may be two approaches for making compliances requiring accounting data.

a. Using same software for accounting and tax compliance; and

b. Using different software for accounting and tax compliance.

Software is needed for tax compliances as almost all the tax compliance today is through electronic mode only. If separate software is used for accounting and tax compliance, we need to put data in tax compliance software either manually or electronically. There are some pros and cons of both the approaches as discussed in the Table 2.10.1.

Table 2.10.1: Pros and Cons of having single software for Accounting and Tax Compliance

S. No.	Particulars	Accounting & Tax Compliance Software	Only Tax Compliance Software
1	**Ease of software operation**	**Less** – as this is integrated system of accounting and tax compliance, everything connected with other and making changes at one place may affect other aspects also.	**More** – as this is used only for one single purpose, i.e. tax compliance, it is less complicated and bound to be easy.
2	**Features and facilities**	**Less** – as this system is not an exclusive system for tax compliance, it may have	**More** – as this is an exclusive and specifically designed system for tax compliance, naturally

		limited features for tax compliance.	more features and facilities shall exist in this system.
3	**Time and efforts required**	**Less** – as this is an integrated system, time required to transfer data to compliance software is zero.	**More** – as this is a separate software, data from accounting software need to put in this for preparation of returns. This may take extra time and efforts.
4	**Accuracy**	**More –** As this is an integrated system and hence accounting data and tax compliance data shall always be same. No need to transfer data to compliance software and reconcile the data.	**Less –** as there are two separate systems, reconciliation with accounting data is needed, and possibility of mismatch of data is always there.
5	**Cost**	**More** – if tax compliance feature is not available in accounting system, getting it customized may require some amount of cost which may be higher than buying separate software.	**Less** – as this is specific purpose software, there shall be less complications and the cost also shall be less.

SUMMARY

A. Integrated & Non-Integrated Systems

Central database is the main characteristics of an ERP system. In case of non-integrated systems, separate database is maintained by each department separately. Central database is accessed by all the departments for their data needs and communication with other departments. Processes are defined and followed in ERP system. ERP system contains different modules for different purposes. These modules are connected to other modules as per requirements. Mismatch of master data and communication gaps between departments / business units are two major problems of non-integrated systems. Data is stored in two parts, master data and transaction data. Master data is that data which is not expected to change frequently. Voucher in manual accounting is a documentary evidence of transaction. In case of software, it also a place, input form where transaction data is input into the system. Grouping of ledgers is extremely important as reports are prepared based on grouping only. Software consists of two parts, front end and back end. Front end is used to interact with user and back end is used to store the data.

B. Business process modules and their integration with financial and accounting systems

Business process modules are developed according to need of specific industries. Various modules like

C. Reporting System and MIS, Data Analytics and Business Intelligence

Business reporting or enterprise reporting is the public reporting of operating and financial data by a business enterprise. With the dramatic expansion of information technology, and the desire for increased competitiveness in corporations, there has been an increase in the use of computing power to produce unified reports which join different views of the enterprise in one place. High-quality reports also promote better internal decision-making.

D. Business Reporting & Fundamentals of XBRL

XBRL (eXtensible Business Reporting Language) is a freely available and global standard for exchanging business information. XBRL is used by Government, Companies, Regulators, Data Providers, Accountants, Analysts and Investors also.

E. Applicable regulatory and compliance requirements

Compliance means conforming to a rule, such as a specification, policy, standard or law. Regulatory compliance is an organization's adherence to laws, regulations, guidelines and specifications relevant to its business. Violations of regulatory compliance regulations often result in legal punishment, including interest, penalty and prosecution in some cases. There may be two types of compliances, General and Specific.

TEST YOUR KNOWLEDGE

Theoretical Questions

1. As an Auditor, prepare a checklist of the questions that you would ask while performing an ERP Audit. (Refer Section 2.4)
2. How do you differentiate between Master Data and Non-Master Data in a computerized accounting system? Give examples. (Refer Section 2.2.3)
3. Determine the reasons for the importance of Business Reporting. Identify the global standard for exchanging business information and discuss it in detail. (Refer Section 2.9.1 and 2.9.2)

4. An enterprise ABC Ltd. intends to acquire software for Accounting as well as Tax compliance. Prepare a list of pros and cons of having single software for Accounting and Tax compliance.

   (Refer Table 2.10.1 under Section 2.10.2)

5. An article joined an Audit firm where he was briefed upon the details of an Accounting Process Flow. Determine the steps involved in the process.

   (Refer Section 2.6.2)

6. Discuss the process involved under Materials Management Module of ERP.

   (Refer Section 2.6.3)

7. What do you understand by the term "Business Intelligence"? Also, discuss its example. (Refer Section 2.8.3)

8. List the benefits of Customer Relationship Management (CRM).

   (Refer Section 2.6.3)

9. As a manager, you are provided a MIS Report about your department's customer service calls. Determine the various criterions that the information in the report should meet so that the information becomes useful for you.

   (Refer Section 2.7.2)

10. Recognize the application areas of Data Analytics in today's world.

    (Refer Section 2.8.1)

11. Explain the ways in which the Regulators can use eXtensible Business Reporting Language (XBRL).

    (Refer Section 2.9.2)

12. Discuss the key features of Controlling Module in an Enterprise Resource Planning (ERP). (Refer Section 2.6.3)

13. State various features of an ERP System. (Refer Section 2.2.7)

Multiple Choice Questions

1. What is not a part of Inventory Master Data?

   (a) Stock Item

   (b) Stock Group

   (c) Salary Structure

(d) Godowns

2. Which of the following is a main characteristic of ERP System?

(a) Separate data maintenance by each department

(b) Centralised Database

(c) No direct inter department communication

(d) None of the above

3. Which of the following is not a benefit of ERP?

(a) Information integration

(b) Reduction of lead-time

(c) Reduction in Cycle Time

(d) Enhanced Quality Costs

4. Which of the following about Back End is false?

(a) Communicates with user directly

(b) Processes the data

(c) Communicates with front end directly

(d) Generates the report

5. XBRL is used by ______________.

(a) Government only

(b) Accountants only

(c) Investors only

(d) All of above

6. If Cash ledger is grouped under indirect income, ________________.

(a) It shall be displayed in profit and loss account

(b) It shall still be considered in balance sheet as it is a cash ledger

(c) Software shall show error message

(d) None of above

7. Which sentence is true about installed software application?

(a) It is installed on the hard disc of the computer of the user

(b) It is installed on the web server

(c) It is installed on cloud

(d) It is installed on a website

8. ________________implementation involves Extract, Transform, and Load (ETL) procedures in coordination with a data warehouse and then using one or more reporting tools.

(a) Business Reporting

(b) Inventory Accounting

(c) Financial Accounting

(d) Payroll Accounting

9. OLAP stands for _________________.

(a) Offline Analytical Processing

(b) Online Analytical Processing

(c) Online Analytical Product

(d) Offline Analytical Product

10. Which of the following is not an attribute of Information?

(a) Availability

(b) Mode and Format

(c) Completeness

(d) Inadequacy

11. If an organization does not want to install Financial Application on its own System, they can use _______ Applications.

(a) Cloud-based

(b) Web

(c) Installed

(d) Mobile

12. In his work place, an employee Mr. X wants to maintain a record of physical receipts of goods purchased from a vendor Mr. G in his Accounting System. Which Voucher type shall he use?

(a) Delivery note

(b) Receipt note

(c) Sales

(d) Purchase

13. In a Three-Tier Architecture, name the layer that is responsible for receiving the inputs for the users and perform certain validations.

(a) Application Layer

(b) Database Layer

(c) Operating System Layer

(d) Network Layer

14. Which of the following transactions are not recorded in the Voucher Type "Contra" of the Accounting System?

(a) Cash deposit in bank

(b) Cash withdrawal in bank

(c) Cash transfer from one location to another

(d) Recording of all types of trading sales by any mode

15. Few years back, to appoint Chairman of TATA GROUP, TATA SONS Ltd., appointed an international human resource consultant to identify suitable candidates for the job. There were three possible candidates selected. This shall be best defined as which part of Human Resource Process?

(a) Recruitment

(b) Selection

(c) Search

(d) Training

Answers

1	(c)	**2**	(b)	**3**	(d)	**4**	(a)	**5**	(d)	**6**	(a)	**7**	(a)
8	(a)	**9**	(b)	**10**	(d)	**11**	(a)	**12**	(b)	**13**	(a)	**14**	(d)
15	(a)												

CHAPTER 3

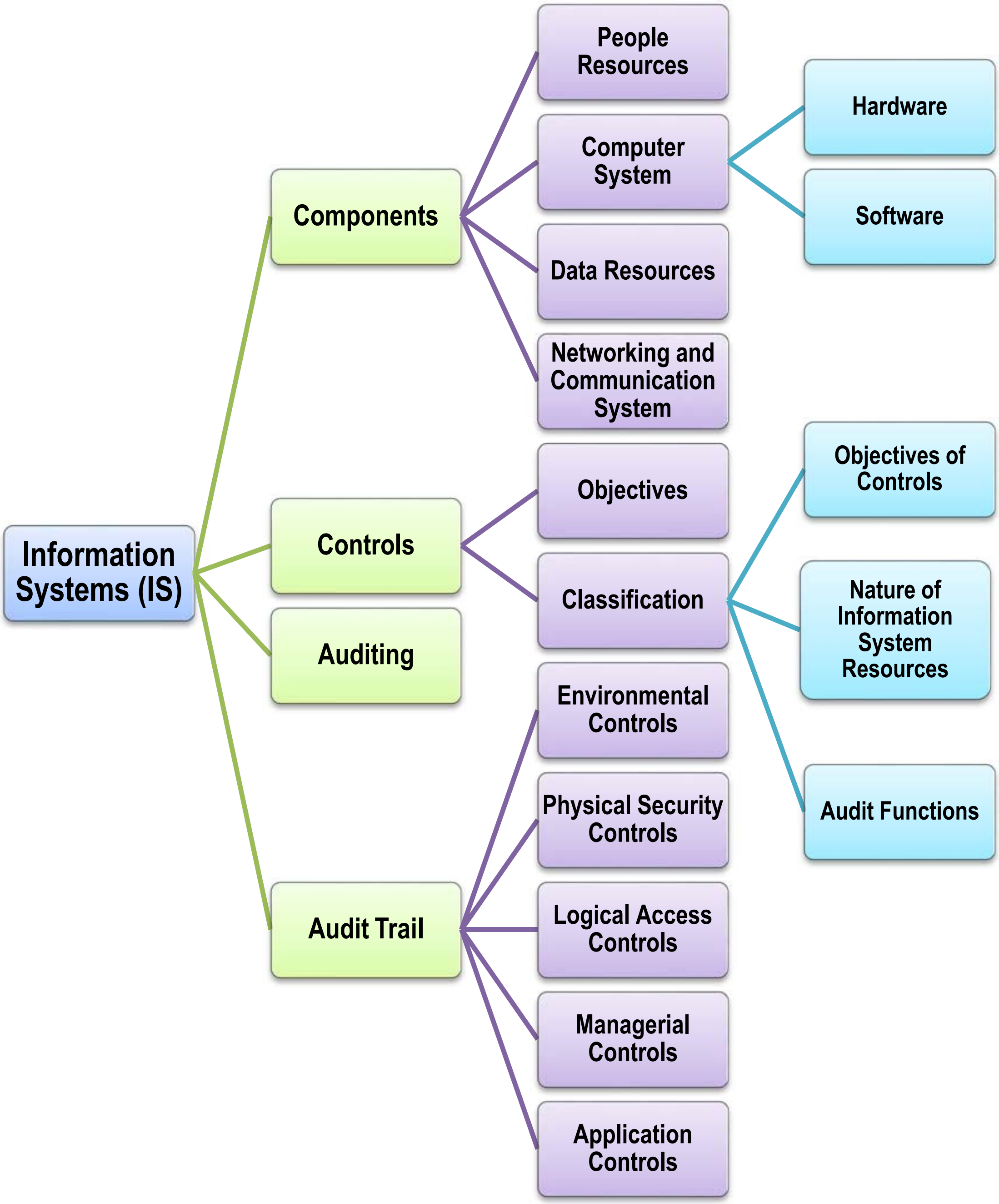
INFORMATION SYSTEMS AND ITS COMPONENTS

LEARNING OUTCOMES

After reading this chapter, you will be able to -

- Understand about working of Financial and Accounting System.
- Comprehend the knowledge about various components of an Information System and its working.
- Appreciate nuances of Application Systems, Operating Systems, Database Systems, Networking and Communication Systems.
- Grasp various types of threats and their mitigating controls to minimize the impact.
- Understand types of controls and audit aspects of various systems.
- Comprehend about an organization structure and individual roles and responsibilities.

CHAPTER OVERVIEW



3.1 INTRODUCTION

Over the past few centuries, the world has moved on from connection amongst individuals to more of connection amongst systems. We now have systems that are constantly exchanging information about various things and even about us, many a times without human intervention. This inter-networking of physical devices, vehicles, smart devices, embedded electronics, software, sensors or any such device is often referred to as IoT (Internet of Things).

What is interesting about various emerging technologies is that at its core we have some key elements, namely, People, Computer Systems (Hardware, Operating System and other Software), Data Resources, Networking and Communication System. In this chapter, we are going to explore each of those key elements.

3.2 INFORMATION SYSTEMS

Information System: Information System (IS) is a combination of people, hardware, software, communication devices, network and data resources that processes (can be storing, retrieving, transforming information) data and information for a specific purpose. The system needs inputs from user (key in instructions and commands, typing, scanning) which will then be processed (calculating, reporting) using technology devices such as computers, and produce output (printing reports, displaying results) that will be sent to another user or other system via a network and a feedback method that controls the operation.

The main aim and purpose of each Information System is to convert the data into information which is useful and meaningful. An Information System depends on the resources of people (end users and IS specialists), hardware (machines and media), software (programs and procedures), data (data and knowledge bases), and networks (communications media and network support) to perform input, processing, output, storage, and control activities that transform data resources into information products. This information system model highlights the relationships among the components and activities of information systems. It also provides a framework that emphasizes four major concepts that can be applied to all types of information systems. An Information System model comprises of following steps:

- **Input:** Data is collected from an organization or from external environments and converted into suitable format required for processing.

- **Process:** A process is a series of steps undertaken to achieve desired outcome or goal. Information Systems are becoming more and more integrated with organizational processes, bringing more productivity and better control to those processes.
- **Output:** Then information is stored for future use or communicated to user after application of respective procedure on it.

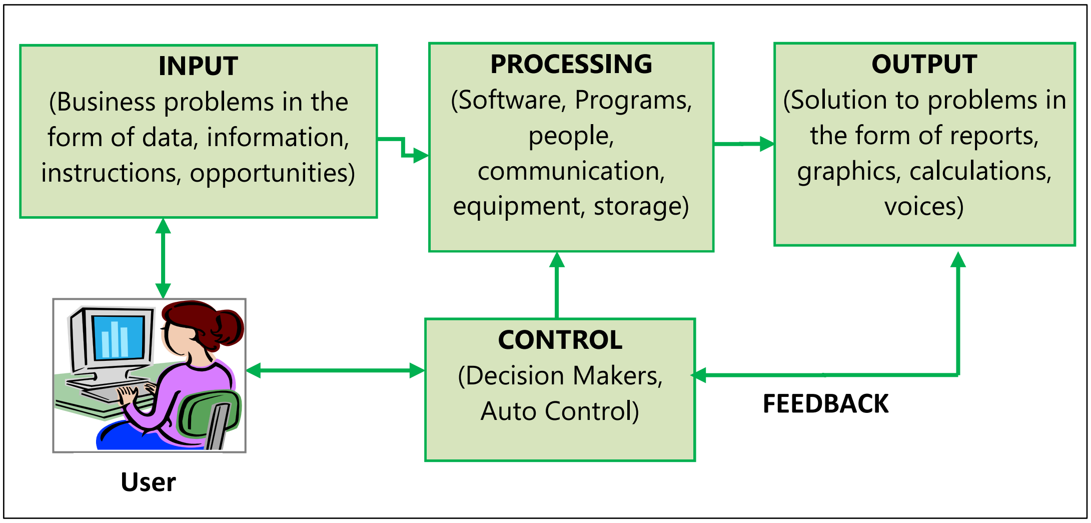

INPUT
(Business problems in the form of data, information, instructions, opportunities)
PROCESSING
(Software, Programs, people, communication, equipment, storage)
OUTPUT
(Solution to problems in the form of reports, graphics, calculations, voices)
CONTROL
(Decision Makers, Auto Control)
FEEDBACK
User

Fig. 3.2.1: Functions of Information Systems

Three basic activities of an information system that are defined above, helps enterprise in making decisions, control operations, analyze problems and create new products or services as an output, as shown in Fig. 3.2.1. Apart from these activities, information systems also need feedback that is returned to appropriate members of the enterprises to help them to evaluate at the input stage.

3.3 COMPONENTS OF INFORMATION SYSTEMS

With the help of information systems, enterprises and individuals can use computers to collect, store, and process, analyze, and distribute information. There are different types of information systems, i.e. Manual (paper and pencil) information system, Informal (word to mouth) information system, Formal (written procedures) information system and Computer based information system. This chapter mainly focuses on computer based information system. A Computer Based Information system is a combination of people, IT and business processes that helps management in taking important decisions to carry out the business successfully.

Information Systems are networks of hardware and software that people and organizations use to create, collect, filter, process and distribute data. Information Systems are interrelated components working together to collect, process, and store and disseminate information to support decision-making, coordination, control, analysis and visualization in an organization. An Information System comprise of **People, Hardware, Software, Data** and **Network** for communication support shown in Fig. 3.3.1.

Here, people mean the IT professionals i.e. system administrator, programmers and end users i.e. the persons, who can use hardware and software for retrieving the desired information. The hardware means the physical components of the computers i.e. server or smart terminals with different configurations like corei3/corei5/corei7 processors etc. and software means the system software (different types of operating systems e.g. UNIX, LINUX, WINDOWS etc.), application software (different type of computer programs designed to perform specific task) and utility software (e.g. tools). The data is the raw fact, which may be in the form of database. The data may be alphanumeric, text, image, video, audio, and other forms. The network means communication media (Internet, Intranet, Extranet etc.).

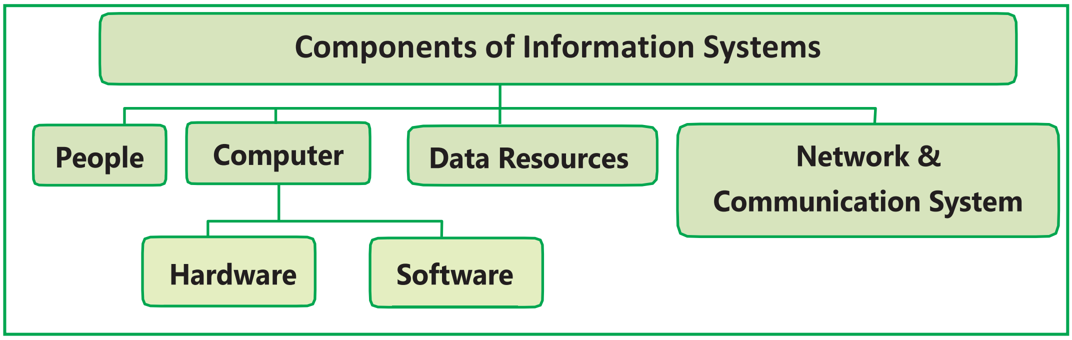

Components of Information Systems
People
Computer
Data Resources
Network & Communication System
Hardware
Software

Fig. 3.3.1: Components of Information Systems

3.3.1 People Resources

While thinking about Information Systems, it is easy to get too focused on the technological components and forget that we must look beyond these tools at the whole picture and try to understand how technology integrates into an organization. A focus on people involved in Information Systems is the next step. From the helpdesk to the system programmers all the way up to the Chief Information Officer (CIO), all of them are essential elements of the information systems. People are the most important element in most Computer-based Information Systems. The people involved include users of the system and information systems personnel, including all the people who manage, run, program, and maintain the system.

In the ever-changing world, innovation is the only key, which can sustain long-run growth. More and more firms are realizing the importance of innovation to gain competitive advantage. Accordingly, they are engaging themselves in various innovative activities. Understanding these layers of information system helps any enterprise grapple with the problems it is facing and innovate to perhaps reduce total cost of production, increase income avenues and increase efficiency of systems.

3.3.2 Computer System – Hardware and Software

Computer System: This is considered as combination of **Hardware & Software**.

Hardware: Information Systems hardware is the part of Information Systems that you can touch-the physical components of technology. Computers, keyboards, hard drives, iPads and flash drives are all examples of Information Systems hardware.

Software: Software is a set of instructions that tells the hardware what to do. Software is not tangible, it cannot be touched. When programmers create software, what they are really doing is simply typing out lists of instructions that tell the hardware what to execute. There are several categories of software, with the two main categories being operating system software, which makes the hardware usable and application software, which does something useful. Examples of operating system software: Microsoft Windows, LINUX, etc. Examples of application software are Microsoft Excel, Adobe Photoshop, Microsoft PowerPoint etc.

I. Hardware

Hardware is the tangible portion of our computer systems; something we can touch and see. It basically consists of devices that perform the functions of input, processing, data storage and output activities of the computer.

(i) **Input Devices** are devices through which we interact with the systems and include devices like Keyboard, Mouse and other pointing devices, Scanners and Bar Code, MICR readers, Webcams, Microphone and Stylus/ Touch Screen. Keyboard helps us with text based input, Mouse helps us in position based input, Scanners & Webcams help in image based input and Microphone helps us in voice based input.

(ii) **Processing Devices** include computer chips that contain the Central Processing Unit and main memory. The Central Processing Unit (CPU or microprocessor) is the actual hardware that interprets and executes the program (software) instructions and coordinates how all the other hardware devices work together. The CPU is built on a small flake of silicon and can contain the equivalent of several million transistors. We can think of transistors as switches which could be "ON" or "OFF" i.e., taking a value of 1 or 0. The processor or CPU is like the brain of the computer.

(iii) **Data Storage Devices** refers to the memory where data and programs are stored. Various types of memory techniques/devices are given as follows:

(a) **Internal Memory:** This includes Processer Registers and Cache Memory.

➢ **Processor Registers:** Registers are internal memory within CPU, which are very fast and very small.

➢ **Cache Memory:** To bridge the huge speed differences between Registers and Primary Memory, we have cache memory. Cache is a smaller, faster memory, which stores copies of the data from the most frequently used main memory locations so that Processor/Registers can access it more rapidly than main memory.

(b) **Primary Memory/Main Memory:** These are devices in which any location can be accessed by the computer's processor in any order (in contrast with sequential order). There are two types of primary memory as discussed in Table 3.3.1:

Table 3.3.1: RAM vs ROM

Random Access Memory (RAM)	**Read Only Memory (ROM)**
Volatile in nature means Information is lost as soon as power is turned off.	Non-volatile in nature (contents remain intact even in absence of power).
Purpose is to hold program and data while they are in use.	Used to store small amount of information for quick reference by CPU.
Information can be read as well as modified.	Information can be read not modified.
Responsible for storing the instructions and data that the computer is using at that present moment.	Generally used by manufacturers to store data and programs like translators that is used repeatedly.

(c) **Secondary Memory:** CPU refers to the main memory for execution of programs, but these main memories are volatile in nature and hence cannot be used to store data on a permanent basis in addition to being small in storage capacity. The secondary memories are available in bigger sizes; thus programs and data can be stored on secondary memories.

Secondary storage differs from primary storage in that it is not directly accessible by the CPU. The features of secondary memory devices are non-volatility (contents are permanent in nature), greater capacity (they are available in large size), greater economy (the cost of these is lesser compared to register and RAMs) and slow speed (slower in speed compared to registers or primary storage).

(d) **Virtual Memory:** Virtual Memory is in fact not a separate device but an imaginary memory area supported by some operating systems (for example, Windows) in conjunction with the hardware. If a computer lacks in required size of the Random-Access Memory (RAM) needed to run a program or operation, Windows uses virtual memory to compensate. Virtual memory combines computer's RAM with temporary space on the hard disk. When RAM runs low, virtual memory moves data from RAM to a space called a paging file. Moving data to and from the paging file frees up RAM to complete its work. Thus, Virtual memory is an allocation of hard disk space to help RAM and depicted in the Fig. 3.3.2.

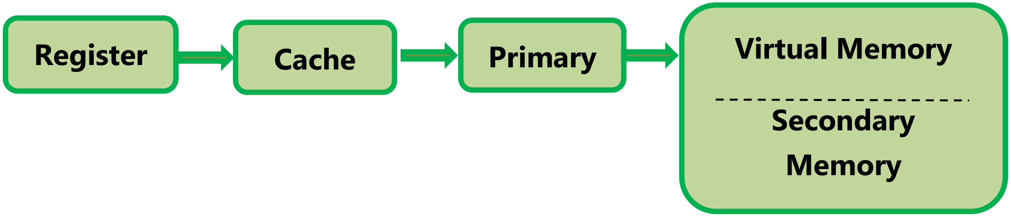


Fig. 3.3.2: Memory Techniques/Devices

(iv) **Output Devices:** Computer systems provide output to decision makers at all levels in an enterprise to solve business problems, the desired output may be in visual, audio or digital forms. Output devices are devices through which system responds. Visual output devices like, a display device visually conveys text, graphics, and video information. Information shown on a display device is called soft copy because the information exists electronically and is displayed for a temporary period. Display devices include CRT monitors, LCD monitors and displays, gas plasma monitors, and televisions. Some types of output are textual, graphical, tactile, audio, and video.

- **Textual output** comprises of characters that are used to create words, sentences, and paragraphs.
- **Graphical outputs** are digital representations of non-text information such as drawings, charts, photographs, and animation.
- **Tactile output** such as raised line drawings may be useful for some individuals who are blind.
- **Audio output** is any music, speech, or any other sound.
- **Video output** consists of images played back at speeds to provide the appearance of full motion.

Most common examples of output devices are Speakers, Headphones, Screen (Monitor), Printer, Voice output communication aid, Automotive navigation system, Video, Plotter, Wireless etc.

II. Software

Software is defined as a set of instructions that tell the hardware what to do. Software is created through the process of programming. Without software, the hardware would not be functional. Software can be broadly divided into two categories: **Operating Systems Software** and **Application Software** as shown in the Fig. 3.3.3. Operating systems manage the hardware and create the interface between the hardware and the user. Application software is the category of programs that do some processing/task for the user.

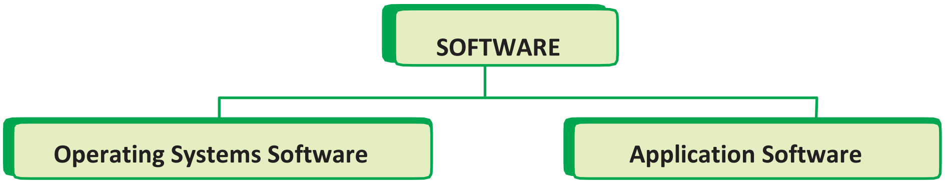


Fig. 3.3.3: Types of Software

(a) Operating Systems Software

An **Operating System (OS)** is a set of computer programs that manages computer hardware resources and acts as an interface with computer applications programs. The operating system is a vital component of the system software in a computer system. Application programs usually require an operating system to function that provides a convenient environment to users for executing their programs. Computer hardware with operating system can thus be viewed as an extended machine, which is more powerful and easy to use. Some prominent Operating systems used nowadays are Windows 7, Windows 8, Linux, UNIX, etc.

All computing devices run an operating system. For personal computers, the most popular operating systems are Microsoft's Windows, Apple's OS X, and different versions of Linux. Smart phones and tablets run operating systems as well, such as Apple's iOS, Google Android, Microsoft's Windows Phone OS, and Research in Motion's Blackberry OS.

A variety of activities are executed by Operating systems which include:

- **Performing hardware functions:** Operating System acts as an intermediary between the application program and the hardware by obtaining input from keyboards, retrieve data from disk and display output on monitors
- **User Interfaces:** Nowadays, Operating Systems are Graphic User Interface (GUI) based which uses icons and menus like in the case of Windows.
- **Hardware Independence:** Operating System provides Application Program Interfaces (API), which can be used by application developers to create application software, thus obviating the need to understand the inner workings of OS and hardware. Thus, OS gives us hardware independence.
- **Memory Management:** Operating System allows controlling how memory is accessed and maximize available memory and storage.
- **Task Management:** This facilitates a user to work with more than one application at a time i.e. multitasking and allows more than one user to use the system i.e. time sharing.
- **Networking Capability:** Operating systems can provide systems with features and capabilities to help connect computer networks like Linux & Windows 8.
- **Logical Access Security:** Operating systems provide logical security by establishing a procedure for identification and authentication using a User ID and Password.
- **File management:** The operating system keeps a track of where each file is stored and who can access it, based on which it provides the file retrieval.

(b) Application Software

As the personal computer proliferated inside organizations, control over the information generated by the organization began splintering. Say the customer service department creates a customer database to keep track of calls and problem reports, and the sales department also creates a database to keep track of customer information. Which one should be used as the master list of customers? As another example, someone in sales might create a spreadsheet to calculate sales revenue, while someone in finance creates a different one that meets the needs of their department. However, it is likely that the two spreadsheets will come up with different totals for revenue. Which one is correct? And who is managing all this information? To resolve these issues, various specific purpose applications were created.

Application software includes all that computer software that causes a computer to perform useful tasks beyond the running of the computer itself. It is a collection of programs which address a real-life problem of its end users which may be business or scientific or any other problem. Application Suite like MS Office 2010 which has MS Word, MS Excel, MS Access, etc.; Enterprise Software like SAP; Content Access Software like Media Players, Adobe Digital etc. are some examples of Application Software.

3.3.3 Data Resources

You can think of data as a collection of facts. For example, your street addresses, the city you live in a new phone number are all pieces of data. Like software, data is also intangible. By themselves, pieces of data are not very useful. But aggregated, indexed and organized together into a database, data can become a powerful tool for businesses. For years' business houses, have been gathering information with regards to customers, suppliers, business partners, markets, cost, and price movement and so on. After collection of information for years' companies have now started analyzing this information and creating important insights out of data. Data is now helping companies to create strategy for future. This is precisely the reason why we have started hearing a lot about data analytics in past few years.

- **Data:** Data, plural of Datum, are the raw bits and pieces of information with no context that can either be quantitative or qualitative. Quantitative data is numeric, the result of a measurement, count, or some other mathematical calculation. Qualitative data is descriptive. "Ruby Red," the color of a 2013 Ford Focus, is an example of qualitative data. By itself, data is not that useful. For it to be useful, it needs to be given context. For example - "15, 23, 14, and 85" are the numbers of students that had registered for upcoming classes that would-be information. Once we have put our data into context, aggregated and analyzed it, we can use it to make decisions for our organization.

- **Database:** A set of logically inter-related organized collection of data is Database. The goal of many Information Systems is to transform data into information to generate knowledge that can be used for decision making. To do this, the system must be able to take data, put the data into context and provide tools for aggregation and analysis.

♦ **Database Management Systems (DBMS):** DBMS may be defined as a software that aid in organizing, controlling and using the data needed by the application programme. They provide the facility to create and maintain a well-organized database. These systems are primarily used to develop and analyze single-user databases and are not meant to be shared across a network or Internet, but are instead installed on a device and work with a single user at a time. Various operations that can be performed on these files are as follows:

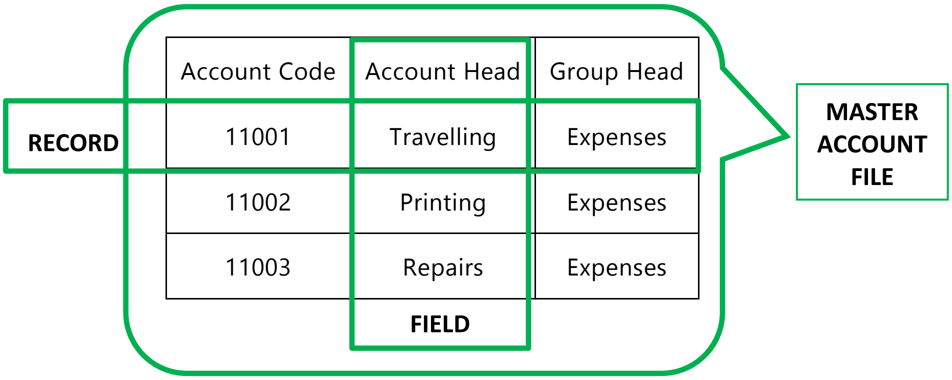
- Adding new files to database,
- Deleting existing files from database,
- Inserting data in existing files,
- Modifying data in existing files,
- Deleting data in existing files, and
- Retrieving or querying data from existing files.

Commercially available Data Base Management Systems are Oracle, MySQL, SQL Servers and DB2 etc. DBMS packages generally provide an interface to view and change the design of the database, create queries, and develop reports. Microsoft Access and Open Office Base are examples of personal DBMS.

♦ **Database Models:** Databases can be organized in many ways, and thus take many forms. A Database Model is a type of data model that determines the logical structure of a database and fundamentally determines in which manner data can be stored, organized and manipulated. Let's now look at the database model hierarchy. Hierarchy of database is as under:

- **Database:** This is a collection of Files/Tables.
- **File or Table:** This is a collection of Records. It is also referred as Entity.
- **Record:** This is a collection of Fields.
- **Field:** This is a collection of Characters, defining a relevant attribute of Table instance.
- **Characters:** These are a collection of Bits.

This hierarchy is shown in the Fig. 3.34:



Account Code	Account Head	Group Head
11001	Travelling	Expenses
11002	Printing	Expenses
11003	Repairs	Expenses

Fig. 3.3.4: Hierarchy of Databases

Some prominent database models are as follows:

A. **Hierarchical Database Model:** In this, records (also known as Nodes) are logically organized into a hierarchy of relationships in an inverted tree pattern. The top parent record in the hierarchy that "own" other records is called Parent Record/ Root Record which may have one or more child records, but no child record may have more than one parent record. Thus, each node is related to the others in a parent-child relationship. Thus, the hierarchical data structure implements one-to-one and one-to-many relationships.

For example, an equipment database, shown in Fig. 3.3.5 may have building records, room records, equipment records, and repair records. The database structure reflects the fact that repairs are made to equipment located in rooms that are part of buildings.

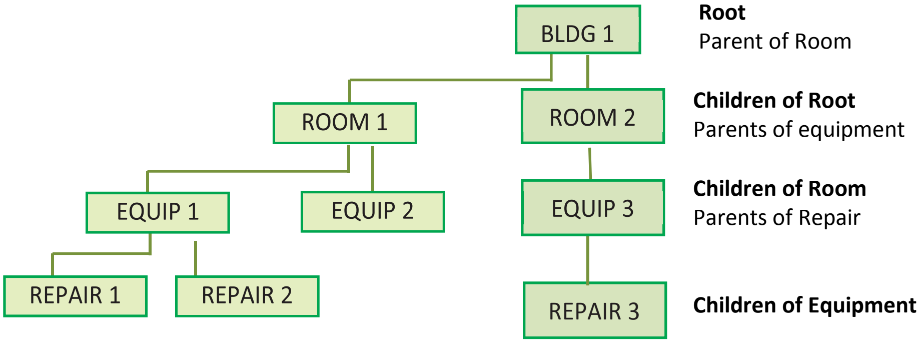


Fig. 3.3.5: Hierarchical Database Model

B. **Network Database Model:** The network model is a variation of the hierarchical model in which unlike the hierarchical model, the branches can be connected to multiple nodes. A network database structure views all records in sets; wherein each set is composed of an owner record and one or more member records thus allowing the network model to implement the many-to-one and the many-to-many relationship types.

For example, suppose that in our database, it is decided to have the following records: Repair vendor records for the companies that repair the equipment, equipment records for the various machines we have, and repair invoice records for the repair bills for the equipment. Suppose four repair vendors have completed repairs on equipment items 1,2,3,4,5,6,7 and 8. These records might be logically organized into the sets shown in Fig. 3.3.6.

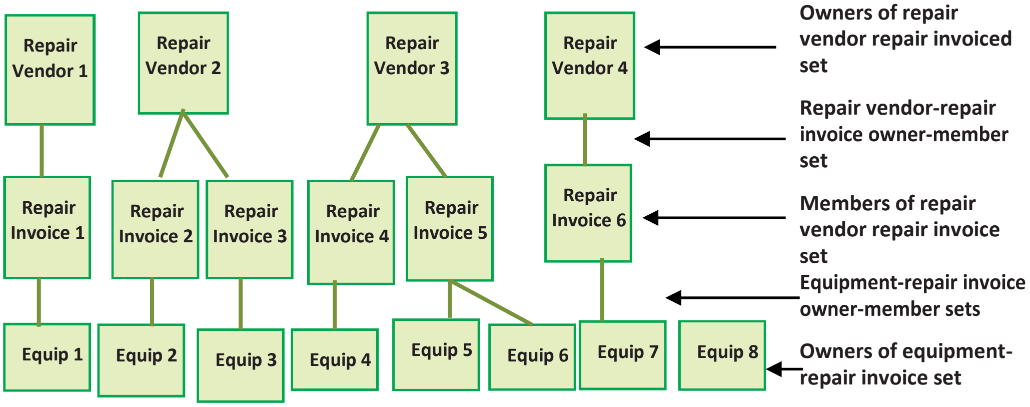


Fig. 3.3.6: Example of Network Database Model

C. **Relational Database Model:** A Relational Database allows the definition of data and their structures, storage and retrieval operations and integrity constraints that can be organized in a Table structure. A table is a collection of records and each record in a table contains the same fields, which define the nature of the data stored in the table. A record is one instance of a set of fields in a table. Three key terms are used extensively in relational database models:

- **Relations:** A relation is a table with columns and rows.
- **Attributes:** The named columns of the relation are called attributes (fields); and
- **Domains:** It is the set of values the attributes can take.

In this, all the tables are related by one or more fields, so that it is possible to connect all the tables in the database through the field(s) they have in common. For each table, one of the fields is identified as a Primary Key, which is the unique identifier for each record in the table. Keys are commonly used to join or combine data from two or more tables. Popular examples of relational databases are Microsoft Access, MySQL, and Oracle.

D. **Object Oriented Data Base Model:** It is based on the concept that the world can be modeled in terms of objects and their interactions. An **Object-Oriented Database** provides a mechanism to store complex data such as images, audio and video, etc. An object-oriented database (also referred to as Object-Oriented Database Management System or OODBMS) is a set of objects. In these databases, the data is modeled and created as objects.

OODBMS helps programmers make objects which are an independently functioning application or program, assigned with a specific task or role to perform. In the Fig. 3.3.7, the light rectangle indicates that 'engineer' is an object possessing attributes like 'date of birth', 'address', etc. which is interacting with another object known as 'civil jobs'. When a civil job is commenced, it updates the 'current job' attribute of the object known as 'engineer', because 'civil job' sends a message to the latter object.

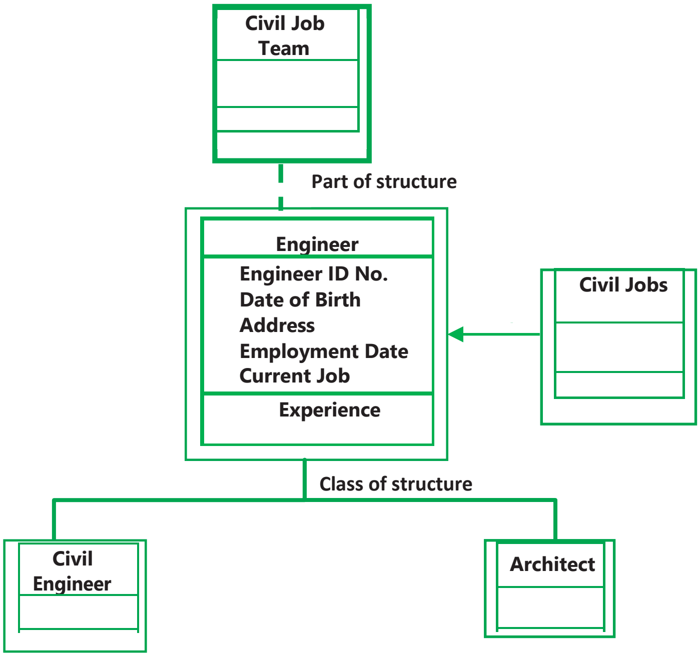


Fig. 3.3.7: An object-oriented database design

(ii) Advantages of DBMS

Major advantages of DBMS are given as follows:

- **Permitting Data Sharing:** One of the principle advantages of a DBMS is that the same information can be made available to different users.
- **Minimizing Data Redundancy:** In a DBMS, duplication of information or redundancy is, if not eliminated, carefully controlled or reduced i.e. there is no need to repeat the same data repeatedly. Minimizing redundancy reduces significantly the cost of storing information on storage devices.
- **Integrity can be maintained:** Data integrity is maintained by having accurate, consistent, and up-to-date data. Updates and changes to the data only must be made in one place in DBMS ensuring Integrity.
- **Program and File consistency:** Using a DBMS, file formats and programs are standardized. The level of consistency across files and programs makes it easier to manage data when multiple programmers are involved as the same rules and guidelines apply across all types of data.
- **User-friendly:** DBMS makes the data access and manipulation easier for the user. DBMS also reduces the reliance of users on computer experts to meet their data needs.
- **Improved security:** DBMS allows multiple users to access the same data resources in a controlled manner by defining the security constraints. Some sources of information should be protected or secured and only viewed by select individuals. Using passwords, DBMS can be used to restrict data access to only those who should see it.
- **Achieving program/data independence:** In a DBMS, data does not reside in applications but data bases program & data are independent of each other.
- **Faster Application Development:** In the case of deployment of DBMS, application development becomes fast. The data is already therein databases, application developer has to think of only the logic required to retrieve the data in the way a user needs.

(iii) Disadvantages of a DBMS

- **Cost:** Implementing a DBMS system in terms of both system and user-training can be expensive and time-consuming, especially in large enterprises. Training requirements alone can be quite costly.

- ♦ **Security:** Even with safeguards in place, it may be possible for some unauthorized users to access the database. If one gets access to database, then it could be an all or nothing proposition.

Some Related Concepts of Database

A. Big Data: A new buzzword that has been capturing the attention of businesses lately is Big Data. The term refers to such massively large data sets that conventional database tools do not have the processing power to analyze them. For example, Flipkart must process over millions of customer transactions every hour during the Billion Day Sale. Storing and analyzing that much data is beyond the power of traditional database-management tools. Understanding the best tools and techniques to manage and analyze these large data sets is a problem that governments and businesses alike are trying to solve. This is an interesting space to explore from a career perspective since everything is nothing more than data. In fact, you and I are nothing more than data points in databases on various companies.

Some examples of industries that use big data analytics include the hospitality industry, healthcare companies, public service agencies, and retail businesses.

Benefits of Big Data Processing are as follows:

a) Ability to process Big Data brings in multiple benefits, such as-

- ***Businesses can utilize outside intelligence while taking decisions.***
- ***Access to social data from search engines and sites like Facebook, Twitter are enabling organizations to fine tune their business strategies.***
- ***Early identification of risk to the product/services, if any***

b) Improved customer service

- ***Traditional customer feedback systems are getting replaced by new systems designed with Big Data technologies. In these new systems, Big Data and natural language processing technologies are being used to read and evaluate consumer responses.***

c) Better operational efficiency

- ***Integration of Big Data technologies and data warehouse helps an organization to offload infrequently accessed data, this leading to better operational efficiency.***

B. Data Warehouse: As organizations, have begun to utilize databases as the centre piece of their operations, the need to fully understand and leverage the data they are collecting has become more and more apparent. However, directly analyzing the data that is needed for day-to-day operations is not a good idea; we do not want to tax the operations of the company more than we need to. Further, organizations also want to analyze data in a historical sense: How does the data we have today compare with the same set of data this time last month, or last year? From these needs arose the concept of the data warehouse.

The concept of the Data Warehouse is simple: **Extract** data from one or more of the organization’s databases and **Load** it into the data warehouse (which is itself another database) for storage and analysis. However, the execution of this concept is not that simple. A data warehouse should be designed so that it meets the following criteria:

- It uses **non-operational data**. This means that the data warehouse is using a copy of data from the active databases that the company uses in its day-to-day operations, so the data warehouse must pull data from the existing databases on a regular, scheduled basis.
- The data is **time-variant**. This means that whenever data is loaded into the data warehouse, it receives a time stamp, which allows for comparisons between different time periods.
- The data is **standardized**. Because the data in a data warehouse usually comes from several different sources, it is possible that the data does not use the same definitions or units. For example, our Events table in our Student Clubs database lists the event dates using the mm/dd/yyyy format (e.g., 01/10/2013). A table in another database might use the format yy/mm/dd (e.g.13/01/10) for dates. For the data warehouse to match up dates a standard date format would have to be agreed upon and all data loaded into the data warehouse would have to be converted to use this standard format. This process is called **Extraction-Transformation-Load (ETL).**
- There are two primary schools of thought when designing a data warehouse: **Bottom-Up** and **Top- Down.**
    - The **Bottom-Up Approach** starts by creating small data warehouses, called data marts, to solve specific business problems. As these data marts are created, they can be combined into a larger data warehouse.
    - The **Top-Down Approach** suggests that we should start by creating an enterprise-wide data warehouse and then, as specific business needs are identified, create smaller data marts from the data warehouse.

❖ Benefits of Data Warehouse

Organizations find data warehouses quite beneficial for several reasons (Refer Fig. 3.3.8):

- The process of developing a data warehouse forces an organization to better understand the data that it is currently collecting and, equally important, what data is not being collected.
- A data warehouse provides a centralized view of all data being collected across the enterprise and provides a means for determining data that is inconsistent.
- Once all data is identified as consistent, an organization can generate one version of the truth. This is important when the company wants to report consistent statistics about itself, such as revenue or number of employees.
- By having a data warehouse, snapshots of data can be taken over time. This creates a historical record of data, which allows for an analysis of trends.
- A data warehouse provides tools to combine data, which can provide new information and analysis.

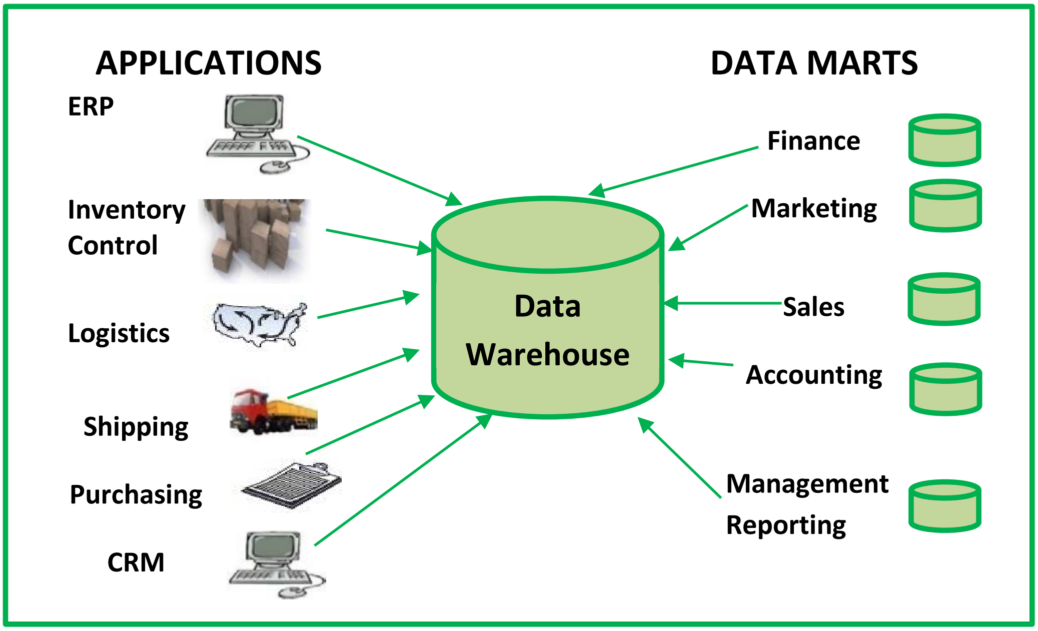


Fig. 3.3.8: Centralized view of Data Warehouse

- **Data Mining:** Data Mining is the process of analysing data to find previously unknown trends, patterns, and associations to make decisions. Generally, data mining is accomplished through automated means against extremely large data sets, such as a data warehouse. An example of data mining includes an analysis of sales from a large grocery chain that might determine that milk is purchased more frequently the day after it rains in cities with a population of less than 50,000. A bank may find that loan applicants whose bank accounts show particular deposit and withdrawal patterns are not good credit risks. A baseball team may find that collegiate baseball players with specific statistics in hitting, pitching, and fielding make for more successful major league players.

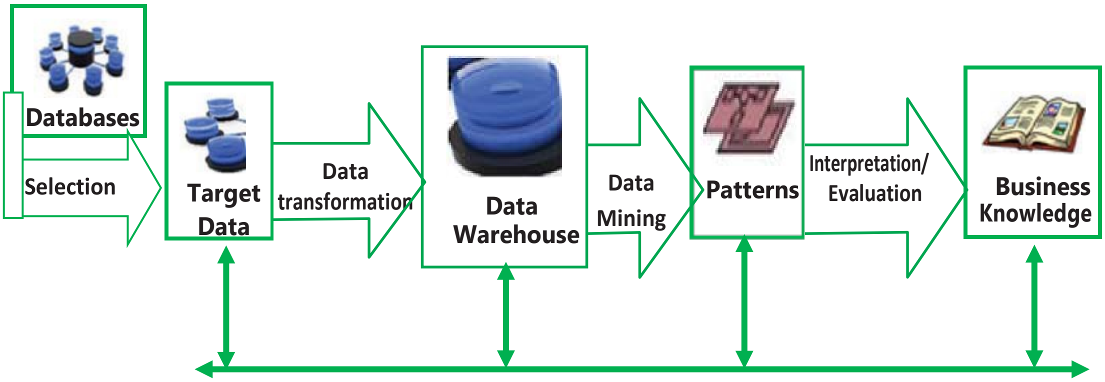


Fig. 3.3.9: Steps involved in Data Mining

The steps involved in the Data Mining process are as follows:

a. **Data Integration:** Firstly, the data are collected and integrated from all the different sources.

b. **Data Selection:** It may be possible that all the data collected may not be required in the first step. So, in this step we select only those data which we think useful for data mining.

c. **Data Cleaning:** The data that is collected are not clean and may contain errors, missing values, noisy or inconsistent data. Thus, we need to apply different techniques to get rid of such anomalies.

d. **Data Transformation:** The data even after cleaning are not ready for mining as it needs to be transformed into an appropriate form for mining using different techniques like - smoothing, aggregation, normalization etc.

e. **Data Mining:** In this, various data mining techniques are applied on the data to discover the interesting patterns. Techniques like clustering and association analysis are among the many different techniques used for data mining.

f. **Pattern Evaluation and Knowledge Presentation:** This step involves visualization, transformation, removing redundant patterns etc. from the patterns we generated.

g. **Decisions / Use of Discovered Knowledge:** This step helps user to make use of the knowledge acquired to take better decisions.

In some cases, a data-mining project is begun with a hypothetical result in mind. For example, a grocery chain may already have some idea that buying patterns change after it rains and want to get a deeper understanding of exactly what is happening. In other cases, there are no presuppositions and a data-mining program is run against large data sets to find patterns and associations. Refer Fig. 3.3.9.

3.3.4 Networking and Communication Systems

In today's high speed world, we cannot imagine an information system without an effective and efficient communication system; which is a valuable resource which helps in good management. Telecommunication networks give an organization the capability to move information rapidly between distant locations and to provide the ability for the employees, customers, and suppliers to collaborate from anywhere, combined with the capability to bring processing power to the point of the application. All of this offers firm important opportunities to restructure its business processes and to capture high competitive ground in the marketplace. Through telecommunications, this value may be:

(i) An increase in the efficiency of operations;

(ii) Improvements in the effectiveness of management; and

(iii) Innovations in the marketplace.

Computer Network is a collection of computers and other hardware interconnected by communication channels that allow sharing of resources and information. Where at least one process in one device can send/receive data to/from at least one process residing in a remote device, then the two devices are said to be in a network. A network is a group of devices connected to each other.

Network and Communication System: These consist of both physical devices and software, links the various pieces of hardware and transfers the data from one physical location to another. Computers and communications equipment can be connected in networks for sharing voice, data, images, sound and video. A network links two or more computers to share data or resources such as a printer.

Every enterprise needs to manage its information in an appropriate and desired manner. The enterprise must do the following for this:

- Knowing its information needs;
- Acquiring that information;
- Organizing that information in a meaningful way;
- Assuring information quality; and
- Providing software tools so that users in the enterprise can access information they require.

Each component, namely the computer in a computer network is called a 'Node'. Computer networks are used for exchange of data among different computers and to share the resources like CPU, I/O devices, storages, etc. without much of an impact on individual systems. In real world, we see numerous networks like Telephone/ mobile network, postal networks etc. If we look at these systems, we can analyze that networks could be of two types:

- **Connection Oriented networks:** Wherein a connection is first established between the sender and the receiver and then data is exchanged like it happens in case of telephone networks.
- **Connectionless Networks:** Where no prior connection is made before data exchanges. Data which is being exchanged in fact has a complete contact information of recipient and at each intermediate destination, it is decided how to proceed further like it happens in case of postal networks.

These real-world networks have helped model computer networks. Each of these networks is modeled to address the following basic issues:

- **Routing:** It refers to the process of deciding on how to communicate the data from source to destination in a network.
- **Bandwidth:** It refers to the amount of data which can be sent across a network in given time.
- **Resilience:** It refers to the ability of a network to recover from any kind of error like connection failure, loss of data etc.

- **Contention:** It refers to the situation that arises when there is a conflict for some common resource in a network. For example, network contention could arise when two or more computer systems try to communicate at the same time.

The following are the important benefits of a computer network:

- **Distributed nature of information:** There would be many situations where information must be distributed geographically. E.g. in the case of Banking Company, accounting information of various customers could be distributed across various branches but to make Consolidated Balance Sheet at the year-end, it would need networking to access information from all its branches.
- **Resource Sharing:** Data could be stored at a central location and can be shared across different systems. Even resource sharing could be in terms of sharing peripherals like printers, which are normally shared by many systems. E.g. In the case of a CBS, Bank data is stored at a Central Data Centre and could be accessed by all branches as well as ATMs.
- **Computational Power:** The computational power of most of the applications would increase drastically if the processing is distributed amongst computer systems. For example: processing in an ATM machine in a bank is distributed between ATM machine and the central Computer System in a Bank, thus reducing load on both.
- **Reliability:** Many critical applications should be available 24x7, if such applications are run across different systems which are distributed across network then the reliability of the application would be high. E.g. In a city, there could be multiple ATM machines so that if one ATM fails, one could withdraw money from another ATM.
- **User communication:** Networks allow users to communicate using e-mail, newsgroups, video conferencing, etc.

Telecommunications may provide these values through the following impacts:

(a) **Time compression:** Telecommunications enable a firm to transmit raw data and information quickly and accurately between remote sites.

(b) **Overcoming geographical dispersion:** Telecommunications enable an organization with geographically remote sites to function, to a degree, as though these sites were a single unit. The firm can then reap benefits of scale and scope which would otherwise be unobtainable.

(c) **Restructuring business relationships:** Telecommunications make it possible to create systems which restructure the interactions of people within a firm as well as a firm's relationships with its customers. Operational efficiency may be raised by eliminating intermediaries from various business processes.

3.4 INFORMATION SYSTEMS' CONTROLS

The increasing use of IT in organizations has made it imperative that appropriate information systems are implemented in an organization. IT should cover all key aspects of business processes of an enterprise and should have an impact on its strategic and competitive advantage for its success. The enterprise strategy outlines the approach, it wishes to formulate with relevant policies and procedures to achieve business objectives. The basic purpose of information system controls in an organization is to ensure that the business objectives are achieved and undesired risk events are prevented, detected and corrected. This is achieved by designing and effective information control framework, which comprise policies, procedures, practices, and organization structure that gives reasonable assurances that the business objectives will be achieved.

Some of the critical control lacking in a computerized environment are as follows:

- Lack of management understanding of IS risks and related controls;
- Absence or inadequate IS control framework;
- Absence of weak general controls and IS controls;
- Lack of awareness and knowledge of IS risks and controls amongst the business users and even IT staff;
- Complexity of implementation of controls in distributed computing environments and extended enterprises;
- Lack of control features or their implementation in highly technology driven environments; and
- Inappropriate technology implementations or inadequate security functionality in technologies implemented.

Internal controls can be classified into various categories to illustrate the interaction of various groups in the enterprise and their effect on information systems on different basis.

These categories have been represented in the Fig. 3.4.1:

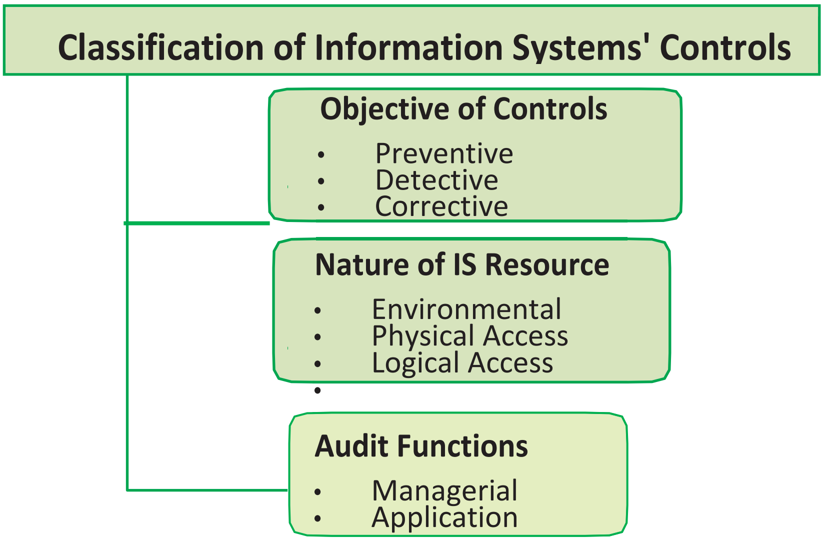


Fig. 3.4.1: Classification of IS Controls

3.4.1 Classification based on "Objective of Controls"

The controls per the time that they act, relative to a security incident can be classified as under:

(A) Preventive Controls: These controls prevent errors, omissions, or security incidents from occurring. Examples include simple data-entry edits that block alphabetic characters from being entered in numeric fields, access controls that protect sensitive data/ system resources from unauthorized people, and complex and dynamic technical controls such as anti-virus software, firewalls, and intrusion prevention systems. In other words, Preventive Controls are those inputs, which are designed to prevent an error, omission or malicious act occurring. Some of the examples of Preventive Controls are as follows:

Any control can be implemented in both manual and computerized environment for the same purpose. Only, the implementation methodology may differ from one environment to the other. Some of the examples of preventive controls can be Employing qualified personnel; Segregation of duties; Access control; Vaccination against diseases; Documentation; Prescribing appropriate books for a course; Training and retraining of staff; Authorization of transaction; Validation, edit checks in the application; Firewalls; Anti-virus software (sometimes this acts like a corrective control also), etc., and Passwords. The above list contains both of manual and computerized, preventive controls.

The following Table 3.4.1 shows how the same purpose is achieved by using manual and computerized controls.

Table 3.4.1: Preventive Controls

Purpose	**Manual Control**	**Computerized Control**
Restrict unauthorized entry into the premises.	Build a gate and post a security guard.	Use access control software, smart card, biometrics, etc.
Restrict unauthorized entry into the software applications.	Keep the computer in a secured location and allow only authorized person to use the applications.	Use access control, viz. User ID, password, smart card, etc.

(B) Detective Controls: These controls are designed to detect errors, omissions or malicious acts that occur and report the occurrence. In other words, Detective Controls detect errors or incidents that elude preventive controls. For example, a detective control may identify account numbers of inactive accounts or accounts that have been flagged for monitoring of suspicious activities. Detective controls can also include monitoring and analysis to uncover activities or events that exceed authorized limits or violate known patterns in data that may indicate improper manipulation. For sensitive electronic communications, detective controls can indicate that a message has been corrupted or the sender's secure identification cannot be authenticated. Some of the examples of Detective Controls are as follows:

Review of payroll reports; Compare transactions on reports to source documents; Monitor actual expenditures against budget; Use of automatic expenditure profiling where management gets regular reports of spend to date against profiled spend; Hash totals; Check points in production jobs; Echo control in telecommunications; Duplicate checking of calculations; Past-due accounts report; The internal audit functions; Intrusion Detection System; Cash counts and bank reconciliation and Monitoring expenditures against budgeted amount.

The main characteristics of such controls are given as follows:

- Clear understanding of lawful activities so that anything which deviates from these is reported as unlawful, malicious, etc.;

- An established mechanism to refer the reported unlawful activities to the appropriate person or group;
- Interaction with the preventive control to prevent such acts from occurring; and
- Surprise checks by supervisor.

(C) Corrective Controls: It is desirable to correct errors, omissions, or incidents once they have been detected. They vary from simple correction of data-entry errors, to identifying and removing unauthorized users or software from systems or networks, to recovery from incidents, disruptions, or disasters. Generally, it is most efficient to prevent errors or detect them as close as possible to their source to simplify correction. These corrective processes also should be subject to preventive and detective controls, because they represent another opportunity for errors, omissions, or falsification.

Corrective controls are designed to reduce the impact or correct an error once it has been detected. Corrective controls may include the use of default dates on invoices where an operator has tried to enter the incorrect date. For example- "Complete changes to IT access lists if individual's role changes" is an example of corrective control. If an accounts clerk is transferred to the sales department as a salesman, his/her access rights to the general ledger and other finance functions should be removed and he/she should be given access only to functions required to perform his sales job.

Some of the other examples of Corrective Controls are submitting corrective journal entries after discovering an error; A Business Continuity Plan (BCP); Contingency planning; Backup procedure; Rerun procedures; Change input value to an application system; and Investigate budget variance and report violations.

The main characteristics of the corrective controls are as follows:

- Minimizing the impact of the threat;
- Identifying the cause of the problem;
- Providing Remedy to the problems discovered by detective controls;
- Getting feedback from preventive and detective controls;
- Correcting error arising from a problem; and
- Modifying the processing systems to minimize future occurrences of the incidents.

3.4.2 Classification based on "Nature of Information System Resources"

These are given as follows:

(A) Environmental Controls: These are the controls relating to IT environment such as power, air-conditioning, Uninterrupted Power Supply (UPS), smoke detection, fire-extinguishers, dehumidifiers etc. Tables 3.4.2 (A,B,C,D) enlist all the environmental exposures related to Fire, Electrical Exposures, Water Damage, and Pollution damage and others with their corresponding controls respectively.

I. Fire: It is a major threat to the physical security of a computer installation.

Table 3.4.2(A): Controls for Fire Exposure

- Both automatic and manual fire alarms may be placed at strategic locations and a control panel may be installed to clearly indicate this.
- Besides the control panel, master switches may be installed for power and automatic fire suppression system. Different fire suppression techniques like Dry-pipe sprinkling systems, water based systems, halon etc., depending upon the situation may be used.
- Manual fire extinguishers can be placed at strategic locations.
- Fireproof Walls; Floors and Ceilings surrounding the Computer Room and Fire Resistant Office Materials such as waste-baskets, curtains, desks, and cabinets should be used.
- Fire exits should be clearly marked. When a fire alarm is activated, a signal may be sent automatically to permanently manned station.
- All staff members should know how to use the system. The procedures to be followed during an emergency should be properly documented are Fire Alarms, Extinguishers, Sprinklers, Instructions / Fire Brigade Nos., Smoke detectors, and Carbon dioxide based fire extinguishers.
- Less Wood and plastic should be in computer rooms.
- Use a gas based fire suppression system.

- To reduce the risk of firing, the location of the computer room should be strategically planned and should not be in the basement or ground floor of a multi-storey building.
- Regular Inspection by Fire Department should be conducted.
- Fire suppression systems should be supplemented and not replaced by smoke detectors.

- **Documented and Tested Emergency Evacuation Plans:** Relocation plans should emphasize human safety, but should not leave information processing facilities physically unsecured. Procedures should exist for a controlled shutdown of the computer in an emergency. In all circumstances saving human life should be given paramount importance.
- **Smoke Detectors:** Smoke detectors are positioned at places above and below the ceiling tiles. Upon activation, these detectors should produce an audible alarm and must be linked to a monitored station (for example, a fire station).
- **Wiring Placed in Electrical Panels and Conduit:** Electrical fires are always a risk. To reduce the risk of such a fire occurring and spreading, wiring should be placed in the fire-resistant panels and conduit. This conduit generally lies under the fire-resistant raised floor in the computer room.

II. Electrical Exposures: These include risk of damages that may be caused due electrical faults. These include non-availability of electricity, spikes (temporary very high voltages), fluctuations of voltage and other such risk.

Table 3.4.2(B): Controls for Electrical Exposure

- The risk of damage due to power spikes can be reduced using Electrical Surge Protectors that are typically built into the Un-interruptible Power System (UPS).
- **Un-interruptible Power System (UPS)/Generator:** In case of a power failure, the UPS provides the back up by providing electrical power from the battery to the computer for a certain span of time. Depending on the sophistication of the UPS, electrical power supply could continue to flow for days or for just a few minutes to permit an orderly computer shutdown.
- Voltage regulators and circuit breakers protect the hardware from temporary increase or decrease of power.
- **Emergency Power-Off Switch:** When the need arises for an immediate power shut down during situations like a computer room fire or an emergency evacuation, an emergency power-off switch at the strategic locations would serve the purpose. They should be easily accessible and yet secured from unauthorized people.

III. Water Damage: Water damage to a computer installation can be the outcome of water pipes burst. Water damage may also result from other resources such as cyclones, tornadoes, floods etc.

Table 3.4.2(C): Controls for Water Exposure

- Wherever possible have waterproof ceilings, walls and floors;
- Ensure an adequate positive drainage system exists;
- Install alarms at strategic points within the installation;
- In flood areas have the installation above the upper floors but not at the top floor;
- Water proofing; and
- Water leakage Alarms.

IV. Pollution Damage and others: The major pollutant in a computer installation is dust. Dust caught between the surfaces of magnetic tape / disk and the reading and writing heads may cause either permanent damage to data or read/ write errors.

Table 3.4.2(D): Controls for Pollution Damage Exposure

Some of the controls are as follows:

- **Power Leads from Two Substations:** Electrical power lines that are exposed to many environmental dangers such as water, fire, lightning, cutting due to careless digging etc. To avoid these types of events, redundant power links should feed into the facility. Interruption of one power supply does not adversely affect electrical supply.
- **Prohibitions against Eating, Drinking and Smoking within the Information Processing Facility:** These activities should be prohibited from the information processing facility. This prohibition should be clear, e.g. a sign on the entry door.

(B) Physical Access Controls: Physical Exposures includes abuse of data processing resources; Blackmail; Embezzlement (an act of dishonestly withholding assets for conversion (theft) of such assets, by one or more persons to whom the assets were entrusted, either to be held or to be used for specific purposes); Damage, vandalism or theft to equipment's or documents; Public disclosure of sensitive information; and Unauthorized entry.

The Physical Access Controls are the controls relating to physical security of the tangible IS resources and intangible resources stored on tangible media etc. Such controls include Access control doors, Security guards, door alarms, restricted entry to secure areas, visitor logged access, CCTV monitoring etc. Refer the Table 3.4.3.

Table 3.4.3: Controls for Physical Exposures

i. **Locks on Doors**

- **Cipher locks (Combination Door Locks)** - Cipher locks are used in low security situations or when many entrances and exits must be usable all the time. To enter, a person presses a four-digit number, and the door will unlock for a predetermined period, usually ten to thirty seconds.
- **Bolting Door Locks** – A special metal key is used to gain entry when the lock is a bolting door lock. To avoid illegal entry, the keys should not be duplicated.
- **Electronic Door Locks** – A magnetic or embedded chip-based plastics card key or token may be entered a reader to gain access in these systems.

ii. **Physical Identification Medium:** These are discussed below:

- **Personal Identification Numbers (PIN):** A secret number will be assigned to the individual, in conjunction with some means of identifying the individual, serves to verify the authenticity of the individual. The visitor will be asked to log on by inserting a card in some device and then enter their PIN via a PIN keypad for authentication. His/her entry will be matched with the PIN number available in the security database.
- **Plastic Cards:** These cards are used for identification purposes. Customers should safeguard their card so that it does not fall into unauthorized hands.
- **Identification Badges:** Special identification badges can be issued to personnel as well as visitors. For easy identification purposes, their color of the badge can be changed. Sophisticated photo IDs can also be utilized as electronic card keys.

iii. **Logging on Facilities:** These are given as under:

- **Manual Logging:** All visitors should be prompted to sign a visitor's log indicating their name, company represented, their purpose of visit, and person to see. Logging may happen at both fronts - reception and entrance to the computer room. A valid and acceptable identification such as a driver's license, business card or vendor identification tag may also be asked for before allowing entry inside the company.
- **Electronic Logging:** This feature is a combination of electronic and biometric security systems. The users logging can be monitored and the unsuccessful attempts being highlighted.

iv. **Other means of Controlling Physical Access:** Other important means of controlling physical access are given as follows:

- **Video Cameras:** Cameras should be placed at specific locations and monitored by security guards. Refined video cameras can be activated by motion. The video supervision recording must be retained for possible future play back.

- **Security Guards:** Extra security can be provided by appointing guards aided with CCTV feeds. Guards supplied by an external agency should be made to sign a bond to protect the organization from loss.
- **Controlled Visitor Access:** A responsible employee should escort all visitors. Visitors may be friends, maintenance personnel, computer vendors, consultants and external auditors.
- **Bonded Personnel:** All service contract personnel, such as cleaning people and off-site storage services, should be asked to sign a bond. This may not be a measure to improve physical security but to a certain extent can limit the financial exposure of the organization.
- **Dead Man Doors:** These systems encompass a pair of doors that are typically found in entries to facilities such as computer rooms and document stations. The first entry door must close and lock, for the second door to operate, with the only one person permitted in the holding area.
- **Non–exposure of Sensitive Facilities**: There should be no explicit indication such as presence of windows of directional signs hinting the presence of facilities such as computer rooms. Only the general location of the information processing facility should be identifiable.
- **Computer Terminal Locks:** These locks ensure that the device to the desk is not turned on or disengaged by unauthorized persons.
- **Controlled Single Entry Point**: All incoming personnel can use controlled Single Entry Point. A controlled entry point is monitored by a receptionist. Multiple entry points increase the chances of unauthorized entry. Unnecessary or unused entry points should be eliminated or deadlocked.
- **Alarm System:** Illegal entry can be avoided by linking alarm system to inactive entry point and the reverse flows of enter or exit only doors, to avoid illegal entry. Security personnel should be able to hear the alarm when activated.
- **Perimeter Fencing:** Fencing at boundary of the facility may also enhance the security mechanism.
- **Control of out of hours of employee-employees:** Employees who are out of office for a longer duration during the office hours should be monitored carefully. Their movements must be noted and reported to the concerned officials frequently.
- **Secured Report/Document Distribution Cart:** Secured carts, such as mail carts, must be covered and locked and should always be attended.

(C) Logical Access Controls: These are the controls relating to logical access to information resources such as operating systems controls, application software boundary controls, networking controls, access to database objects, encryption controls etc. Logical access controls are implemented to ensure that access to systems, data and programs is restricted to authorized users to safeguard information against unauthorized use, disclosure or modification, damage or loss. The key factors considered in designing logical access controls include confidentiality and privacy requirements, authorization, authentication and incident handling, reporting and follow-up, virus prevention and detection, firewalls, centralized security administration, user training and tools for monitoring compliance, intrusion testing and reporting. Logical access controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted. Table 3.4.4 provides the list of Technical Exposures.

Table 3.4.4: Technical Exposures

Technical Exposures: Technical exposures include unauthorized implementation or modification of data and software. Technical exposures include the following:

- **Data Diddling:** This involves the change of data before or after they entered the system. A limited technical knowledge is required to data diddle and the worst part with this is that it occurs before computer security can protect the data.
- **Bomb:** Bomb is a piece of bad code deliberately planted by an insider or supplier of a program. An event, which is logical, triggers a bomb or time based. The bombs explode when the conditions of explosion get fulfilled causing the damage immediately. However, these programs cannot infect other programs. Since, these programs do not circulate by infecting other programs; chances of a widespread epidemic are relatively low.
- **Christmas Card:** It is a well-known example of Trojan and was detected on internal E-mail of IBM system. On typing the word 'Christmas', it will draw the Christmas tree as expected, but in addition, it will send copies of similar output to all other users connected to the network. Because of this message on other terminals, other users cannot save their half-finished work.
- **Worm:** A worm does not require a host program like a Trojan to relocate itself. Thus, a Worm program copies itself to another machine on the network. Since, worms are stand-alone programs, and they can be detected easily in comparison to Trojans and computer viruses. Examples of worms are Existential Worm, Alarm clock Worm etc. The Alarm Clock worm places wake-up calls on a list of users. It passes through the network to an outgoing terminal while the sole purpose of existential worm is to remain alive. Existential worm does not cause damage to the system, but only copies itself to several places in a computer network.
- **Rounding Down:** This refers to rounding of small fractions of a denomination and transferring these small fractions into an authorized account. As the amount is small, it gets rarely noticed.

- **Salami Techniques:** This involves slicing of small amounts of money from a computerized transaction or account. A Salami technique is slightly different from a rounding technique in the sense a fix amount is deducted. For example, in the rounding off technique, ₹ 21,23,456.39 becomes ₹ 21,23,456.40, while in the Salami technique the transaction amount ₹ 21,23,456.39 is truncated to either ₹ 21,23,456.30 or ₹21,23,456.00, depending on the logic.
- **Trap Doors:** Trap doors allow insertion of specific logic, such as program interrupts that permit a review of data. They also permit insertion of unauthorized logic.
- **Spoofing:** A spoofing attack involves forging one's source address. One machine is used to impersonate the other in spoofing technique. Spoofing occurs only after a particular machine has been identified as vulnerable. A penetrator makes the user think that s/he is interacting with the operating system. For example, a penetrator duplicates the login procedure, captures the user's password, attempts for a system crash and makes user login again.

Asynchronous Attacks

They occur in many environments where data can be moved synchronously across telecommunication lines. Data that is waiting to be transmitted are liable to unauthorized access called **Asynchronous Attack**. These attacks are hard to detect because they are usually very small pin like insertions and are of following types:

- **Data Leakage:** This involves leaking information out of the computer by means of dumping files to paper or stealing computer reports and tape.
- **Subversive Attacks:** These can provide intruders with important information about messages being transmitted and the intruder may attempt to violate the integrity of some components in the sub-system.
- **Wire- Tapping:** This involves spying on information being transmitted over communication network.
- **Piggybacking:** This is the act of following an authorized person through a secured door or electronically attaching to an authorized telecommunication link that intercepts and alters transmissions. This involves intercepting communication between the operating system and the user and modifying them or substituting new messages.

Fig. 3.4.2: Asynchronous Attacks

Compromise or absence of logical access controls in the organizations may result in potential losses due to exposures that may lead to the total shutdown of the computer functions. Intentional or accidental exposures of logical access control encourage technical exposures and computer crimes in Table 3.4.4 and Fig. 3.4.2 respectively.

Logical Access Violators are often the same people who exploit physical exposures, although the skills needed to exploit logical exposures are more technical and complex. They are mainly as follows:

- Hackers: Hackers try their best to overcome restrictions to prove their ability. Ethical hackers most likely never try to misuse the computer intentionally;
- Employees (authorized or unauthorized);
- IS Personnel: They have easiest to access to computerized information since they come across to information during discharging their duties. Segregation of duties and supervision help to reduce the logical access violations;
- Former Employees: should be cautious of former employees who have left the organization on unfavorable terms;
- End Users; Interested or Educated Outsiders; Competitors; Foreigners; Organized Criminals; Crackers; Part-time and Temporary Personnel; Vendors and consultants; and Accidental Ignorant – Violation done unknowingly.

Some of the Logical Access Controls are listed below:

I. **User Access Management:** This is an important factor that involves following:

  - **User Registration:** Information about every user is documented. Some questions like why and who is the user granted the access; has the data owner approved the access, and has the user accepted the responsibility? etc. are answered. The de-registration process is also equally important.
  - **Privilege management:** Access privileges are to be aligned with job requirements and responsibilities and are to be minimal w.r.t their job functions. For example, an operator at the order counter shall have direct access to order processing activity of the application system.
  - **User password management:** Passwords are usually the default screening point for access to systems. Allocations, storage, revocation, and reissue of password are password management functions. Educating users is a critical component about passwords, and making them responsible for their password.
  - **Review of user access rights:** A user's need for accessing information changes with time and requires a periodic review of access rights to check anomalies in the user's current job profile, and the privileges granted earlier.

II. **User Responsibilities:** User awareness and responsibility are also important factors and are as follows:

  - **Password use:** Mandatory use of strong passwords to maintain confidentiality.
  - **Unattended user equipment:** Users should ensure that none of the equipment under their responsibility is ever left unprotected. They should also secure their PCs with a password and should not leave it accessible to others.

III. **Network Access Control:** An Internet connection exposes an organization to the harmful elements of the outside world. The protection can be achieved through the following means:

- **Policy on use of network services:** An enterprise wide policy applicable to internet service requirements aligned with the business need for using the Internet services is the first step. Selection of appropriate services and approval to access them should be part of this policy.
- **Enforced path:** Based on risk assessment, it is necessary to specify the exact path or route connecting the networks; e.g. internet access by employees will be routed through a firewall and proxy.
- **Segregation of networks:** Based on the sensitive information handling function; say a VPN connection between a branch office and the head-office, this network is to be isolated from the internet usage service
- **Network connection and routing control:** The traffic between networks should be restricted, based on identification of source and authentication access policies implemented across the enterprise network facility.
- **Security of network services:** The techniques of authentication and authorization policy should be implemented across the organization's network.
- **Firewall:** A Firewall is a system that enforces access control between two networks. To accomplish this, all traffic between the external network and the organization's Intranet must pass through the firewall that will allow only authorized traffic between the organization and the outside to pass through it. The firewall must be immune to penetrate from both outside and inside the organization. In addition to insulating the organization's network from external networks, firewalls can be used to insulate portions of the organization's Intranet from internal access also.
- **Encryption:** Encryption is the conversion of data into a secret code for storage in databases and transmission over networks. The sender uses an encryption algorithm with a key to convert the original message called the Clear text into Cipher text. This is decrypted at the receiving end. Two general approaches are used for encryption viz. private key and public key encryption.
- **Call Back Devices:** It is based on the principle that the key to network security is to keep the intruder off the Intranet rather than imposing security measure after the criminal has connected to the intranet. The call-back device requires the user to enter a password and then the system breaks the connection. If the caller is authorized, the call back device dials

the caller's number to establish a new connection. This limits access only from authorized terminals or telephone numbers and prevents an intruder masquerading as a legitimate user. This also helps to avoid the call forwarding and man-in-the middle attack.

IV. **Operating System Access Control:** Operating System(O/S) is the computer control program that allows users and their applications to share and access common computer resources, such as processor, main memory, database and printers. Major tasks of O/S are Job Scheduling; Managing Hardware and Software Resources; Maintaining System Security; Enabling Multiple User Resource Sharing; Handling Interrupts and Maintaining Usage Records. Operating system security involves policy, procedure and controls that determine, 'who can access the operating system,' 'which resources they can access', and 'what action they can take'. Hence, protecting operating system access is extremely crucial and can be achieved using following steps.

- **Automated terminal identification:** This will help to ensure that a specified session could only be initiated from a certain location or computer terminal.
- **Terminal log-in procedures:** A log-in procedure is the first line of defense against unauthorized access as it does not provide unnecessary help or information, which could be misused by an intruder. When the user initiates the log-on process by entering user-id and password, the system compares the ID and password to a database of valid users and accordingly authorizes the log-in.
- **Access Token:** If the log on attempt is successful, the Operating System creates an access token that contains key information about the user including user-id, password, user group and privileges granted to the user. The information in the access token is used to approve all actions attempted by the user during the session.
- **Access Control List:** This list contains information that defines the access privileges for all valid users of the resource. When a user attempts to access a resource, the system compasses his or her user-id and privileges contained in the access token with those contained in the access control list. If there is a match, the user is granted access.
- **Discretionary Access Control:** The system administrator usually determines; who is granted access to specific resources and maintains the access control list. However, in distributed systems, resources may be controlled by the end-user. Resource owners in this setting may be

granted discretionary access control, which allows them to grant access privileges to other users. For example, the controller who is owner of the general ledger grants read only privilege to the budgeting department while accounts payable manager is granted both read and write permission to the ledger.

- **User identification and authentication:** The users must be identified and authenticated in a foolproof manner. Depending on risk assessment, more stringent methods like Biometric Authentication or Cryptographic means like Digital Certificates should be employed.
- **Password management system:** An operating system could enforce selection of good passwords. Internal storage of password should use one-way hashing algorithms and the password file should not be accessible to users.
- **Use of system utilities:** System utilities are the programs that help to manage critical functions of the operating system e.g. addition or deletion of users. Obviously, this utility should not be accessible to a general user. Use and access to these utilities should be strictly controlled and logged.
- **Duress alarm to safeguard users:** If users are forced to execute some instruction under threat, the system should provide a means to alert the authorities.
- **Terminal time out:** Log out the user if the terminal is inactive for a defined period. This will prevent misuse in absence of the legitimate user.
- **Limitation of connection time:** Define the available time slot. Do not allow any transaction beyond this time. For example, no computer access after 8.00 p.m. and before 8.00 a.m. or on a Saturday or Sunday.

V. Application and Monitoring System Access Control: Some steps are as follows:

- **Information Access restriction:** The access to information is prevented by application specific menu interfaces, which limit access to system function. A user can access only to those items, s/he is authorized to access. Controls are implemented on the access rights of users. For example - read, write, delete, and execute. And ensure that sensitive output is sent only to authorized terminals and locations.
- **Sensitive System isolation:** Based on the critical constitution of a system in an enterprise, it may even be necessary to run the system in an isolated environment. Monitoring system access and use is a detective control, to

check if preventive controls discussed so far are working. If not, this control will detect and report any unauthorized activities.

- **Event logging:** In Computer systems, it is easy and viable to maintain extensive logs for all types of events. It is necessary to review if logging is enabled and the logs are archived properly. An intruder may penetrate the system by trying different passwords and user ID combinations. All incoming and outgoing requests along with attempted access should be recorded in a transaction log. The log should record the user ID, the time of the access and the terminal location from where the request has been originated.
- **Monitor System use:** Based on the risk assessment, a constant monitoring of some critical systems is essential. Define the details of types of accesses, operations, events and alerts that will be monitored. The extent of detail and the frequency of the review would be based on criticality of operation and risk factors. The log files are to be reviewed periodically and attention should be given to any gaps in these logs.
- **Clock Synchronization:** Event logs maintained across an enterprise network plays a significant role in correlating an event and generating report on it. Hence, the need for synchronizing clock time across the network as per a standard time is mandatory.

VI. ***<u>Controls when mobile</u>: In today's organizations, computing facility is not restricted to a certain data center alone. Ease of access on the move provides efficiency and results in additional responsibility on the management to maintain information security. Theft of data carried on the disk drives of portable computers is a high-risk factor. Both physical and logical access to these systems is critical. Information is to be encrypted and access identifications like fingerprint, eye-iris, and smart cards are necessary security features.***

3.4.3 Classification based on "Audit Functions"

Auditors might choose to factor systems in several different ways. Auditors have found two ways to be especially useful when conducting information systems audits. These are discussed below:

A. Managerial Controls: In this part, we shall examine controls over the managerial controls that must be performed to ensure the development, implementation, operation and maintenance of information systems in a planned and controlled manner in an organization. The controls at this level provide a stable infrastructure in which information systems can be built, operated, and maintained on a day-to-day basis.

I. Top Management and Information Systems Management Controls

The controls adapted by the management of an enterprise are to ensure that the information systems function correctly and they meet the strategic business objectives. The management has the responsibility to determine whether the controls that the enterprise system has put in place are sufficient to ensure that the IT activities are adequately controlled. The scope of control here includes framing high-level IT policies, procedures and standards on a holistic view and in establishing a sound internal controls framework within the organization. The high-level policies establish a framework on which the controls for lower hierarchy of the enterprise. The controls flow from the top of an organization to down; the responsibility still lies with the senior management. Top management is responsible for preparing a master plan for the information systems function. The senior managers who take responsibility for IS function in an organization face many challenges. The major functions that a senior manager must perform are Planning, Organizing, Leading and Controlling.

(a) **Planning –** This includes determining the goals of the information systems function and the means of achieving these goals. The steering committee shall comprise of representatives from all areas of the business, and IT personnel that would be responsible for the overall direction of IT. The steering committee should assume overall responsibility for the activities of the information systems function.

(b) **Organizing –** There should be a prescribed IT organizational structure with documented roles and responsibilities and agreed job descriptions. This includes gathering, allocating, and coordinating the resources needed to accomplish the goals that are established during Planning function.

(c) **Leading –** This includes motivating, guiding, and communicating with personnel. The purpose of leading is to achieve the harmony of objectives; ie.. a person's or group's objectives must not conflict with the organization's objectives. The process of leading requires managers to motivate subordinates, direct them and communicate with them.

(d) **Controlling –** This includes comparing actual performance with planned performance as a basis for taking any corrective actions that are needed. This involves determining when the actual activities of the information system's functions deviate from the planned activities.

II. Systems Development Management Controls

Systems Development Management has responsibility for the functions concerned with analyzing, designing, building, implementing, and maintaining information systems. System development controls are targeted to ensure that proper documentations and authorizations are available for each phase of the system development process. It includes controls at controlling new system development activities. The activities discussed below deal with system development controls in IT setup.

- **System Authorization Activities:** All systems must be properly and formally authorized to ensure their economic justification and feasibility. This requires that each new system request be submitted in written form by users to systems professionals who have both the expertise and authority to evaluate and approve (or reject) the request.
- **User Specification Activities:** Users must be actively involved in the systems development process wherein a detailed written descriptive document of the logical needs of the users is created.
- **Technical Design Activities:** The technical design activities translate the user specifications into a set of detailed technical specifications of a system that meets the user's needs.
- **Internal Auditor's Participation:** The internal auditor should be involved at the inception of the system development process to make conceptual suggestions regarding system requirements and controls and should be continued throughout all phases of the development process and into the maintenance phase.
- **Program Testing:** All program modules must be thoroughly tested before they are implemented. The results of the tests are then compared against predetermined results to identify programming and logic errors.
- **User Test and Acceptance Procedures:** Just before implementation, the individual modules of the system must be tested as a unified whole. A test team comprising user personnel, systems professionals, and internal audit personnel subjects the system to rigorous testing. Once the test team is satisfied that the system meets its stated requirements, the system is formally accepted by the user department(s).

III. Programming Management Controls

Program development and implementation is a major phase within the systems development life cycle. The primary objectives of this phase are to produce or acquire and to implement high-quality programs. The Control phase runs in parallel for all other phases during software development or acquisition is to monitor progress against plan and to ensure software released for production use is authentic, accurate, and complete. Refer Table 3.4.5.

Table 3.4.5: Phases of Program Development Life Cycle

Phase	Controls
Planning	Techniques like Work Breakdown Structures (WBS), Gantt charts and PERT (Program Evaluation and Review Technique) Charts can be used to monitor progress against plan.
Control	The Control phase has two major purposes: ♦ Task progress in various software life-cycle phases should be monitored against plan and corrective action should be taken in case of any deviations ♦ Control over software development, acquisition, and implementation tasks should be exercised to ensure software released for production use is authentic, accurate, and complete.
Design	A systematic approach to program design, such as any of the structured design approaches or object-oriented design is adopted.
Coding	Programmers must choose a module implementation and integration strategy (like Top-down, Bottom-up & Threads approach), a coding strategy (that follows percepts of structured programming), and a documentation strategy (to ensure program code is easily readable & understandable).
Testing	Three types of testing can be undertaken: ♦ **Unit Testing –** which focuses on individual program modules; ♦ **Integration Testing –** Which focuses in groups of program modules; and ♦ **Whole-of-Program Testing** – which focuses on whole program. These tests are to ensure that a developed or acquired program achieves its specified requirements.
Operation and Maintenance	Management establishes formal mechanisms to monitor the status of operational programs so maintenance needs can be identified on a timely basis. Three types of maintenance can be used are as follows: ♦ **Repair Maintenance –** in which program errors are corrected; ♦ **Adaptive Maintenance –** in which the program is modified to meet changing user requirements; and ♦ **Perfective Maintenance -** in which the program is tuned to decrease the resource consumption.

IV. Data Resource Management Controls

Many organizations now recognize that data is a critical resource that must be managed properly and therefore, accordingly, centralized planning and control are implemented. For data to be managed better; users must be able to share data;

data must be available to users when it is needed, in the location where it is needed, and in the form in which it is needed. Further it must be possible to modify data easily and the integrity of the data be preserved. If data repository system is used properly, it can enhance data and application system reliability. It must be controlled carefully, however, because the consequences are serious if the data definition is compromised or destroyed. Careful control should be exercised over the roles by appointing senior, trustworthy persons, separating duties to the extent possible and maintaining and monitoring logs of the data administrator's and database administrator's activities.

V. Quality Assurance Management Controls

Quality Assurance management is concerned with ensuring that the –

- Information systems produced by the information systems function achieve certain quality goals; and
- Development, implementation, operation and maintenance of Information systems comply with a set of quality standards.

Quality Assurance (QA) personnel should work to improve the quality of information systems produced, implemented, operated, and maintained in an organization. They perform a monitoring role for management to ensure that –

- Quality goals are established and understood clearly by all stakeholders; and
- Compliance occurs with the standards that are in place to attain quality information systems.

VI. Security Management Controls

Information security administrators are responsible for ensuring that information systems assets categorized under Personnel, Hardware, Facilities, Documentation, Supplies Data, Application Software and System Software are secure. Assets are secure when the expected losses that will occur over some time, are at an acceptable level. The control's classification based on "Nature of Information System Resources – Environmental Controls, Physical Controls and Logical Access Controls are all security measures against the possible threats. However, despite the controls on place, there could be a possibility that a control might fail. Disasters are events / incidents that are so critical that has capability to hit business continuity of an entity in an irreversible manner.

When disaster strikes, it still must be possible to recover operations and mitigate losses using the last resort controls - A Disaster Recovery Plan (DRP) and Insurance. A comprehensive DRP comprise four parts – **an Emergency Plan, a Backup Plan,** a **Recovery Plan** and a **Test Plan.** The plan lays down the policies, guidelines, and procedures for all Information System personnel. Adequate insurance must be able to replace Information Systems assets and to cover the extra costs associated with restoring normal operations.

BCP (Business Continuity Planning) Controls: These controls are related to having an operational and tested IT continuity plan, which is in line with the overall business continuity plan, and its related business requirements to make sure IT services are available as required and to ensure a minimum impact on business in the event of a major disruption

VIII. Operations Management Controls

Operations management is responsible for the daily running of hardware and software facilities. Operations management typically performs controls over the functions as below:

(a) **Computer Operations:** The controls over computer operations govern the activities that directly support the day-to-day execution of either test or production systems on the hardware/software platform available.

(b) **Network Operations:** This includes the proper functioning of network operations and monitoring the performance of network communication channels, network devices, and network programs and files. Data may be lost or corrupted through component failure.

(c) **Data Preparation and Entry:** Irrespective of whether the data is obtained indirectly from source documents or directly from, say, customers, keyboard environments and facilities should be designed to promote speed and accuracy and to maintain the wellbeing of keyboard operators.

(d) **Production Control:** This includes the major functions like- receipt and dispatch of input and output; job scheduling; management of service-level agreements with users; transfer pricing/charge-out control; and acquisition of computer consumables.

(e) **File Library:** This includes the management of an organization's machine-readable storage media like magnetic tapes, cartridges, and optical disks.

(f) **Documentation and Program Library:** This involves that documentation librarians ensure that documentation is stored securely; that only authorized personnel gain access to documentation; that documentation is kept up-to-date and that adequate backup exists for documentation. The documentation may include reporting of responsibility and authority of each function; Definition of responsibilities and objectives of each functions; Reporting responsibility and authority of each function; Policies and procedures; Job descriptions and Segregation of Duties.

(g) **Help Desk/Technical support:** This assists end-users to employ end-user hardware and software such as micro-computers, spreadsheet packages, database management packages etc. and provided the technical support for production systems by assisting with problem resolution.

(h) **Capacity Planning and Performance Monitoring:** Regular performance monitoring facilitates the capacity planning wherein the resource deficiencies must be identified well in time so that they can be made available when they are needed.

(i) **Management of Outsourced Operations:** This has the responsibility for carrying out day-to-day monitoring of the outsourcing contract.

B. Application Controls and their Categories

The objective of application controls is to ensure that data remains complete, accurate and valid during its input, update and storage. The specific controls could include form design, source document controls, input, processing and output controls, media identification, movement and library management, data back-up and recovery, authentication and integrity, legal and regulatory requirements. Any function or activity that works to ensure the processing accuracy of the application can be considered an application control. For example, a counter clerk at a bank is required to perform various business activities as part of his/her job description and assigned responsibilities. S/he can relate to the advantages of technology when he is able to interact with the computer system from the perspective of meeting his job objectives.

I. Boundary Controls: The major controls of the boundary system are the access control mechanisms that links the authentic users to the authorized resources, they are permitted to access. The boundary subsystem establishes the interface between the would-be user of a computer system and the computer itself. Major Boundary Control are as follows:

- **Cryptography:** It deals with programs for transforming data into cipher text that are meaningless to anyone, who does not possess the authentication to access the respective system resource or file. A cryptographic technique encrypts data (clear text) into cryptograms (cipher text) and its strength depends on the time and cost to decipher the cipher text by a cryptanalyst. Three techniques of cryptography are transposition (permute the order of characters within a set of data), substitution (replace text with a key-text) and product cipher (combination of transposition and substitution).

- **Passwords:** User identification by an authentication mechanism with personal characteristics like name, birth date, employee code, function, designation or a combination of two or more of these can be used as a password boundary access control.
- **Personal Identification Numbers (PIN):** PIN is similar to a password assigned to a user by an institution a random number stored in its database independent to a user identification details, or a customer selected number. Hence, a PIN may be exposed to vulnerabilities while issuance or delivery, validation, transmission and storage.
- **Identification Cards:** Identification cards are used to store information required in an authentication process. These cards are to be controlled through the application for a card, preparation of the card, issue, use and card return or card termination phases.
- **Biometric Devices:** Biometric identification e.g. thumb and/or finger impression and eye retina etc. are used as boundary control techniques.

II. Input Controls: Data that is presented to an application as input data must be validated for authorization, reasonableness, completeness, and integrity. These controls are responsible for ensuring the accuracy and completeness of data and instruction input into an application system. Input controls are important and critical since substantial time is spent on input of data, involve human intervention and are, therefore error and fraud prone. These are of following types as shown in the Fig. 3.4.3:

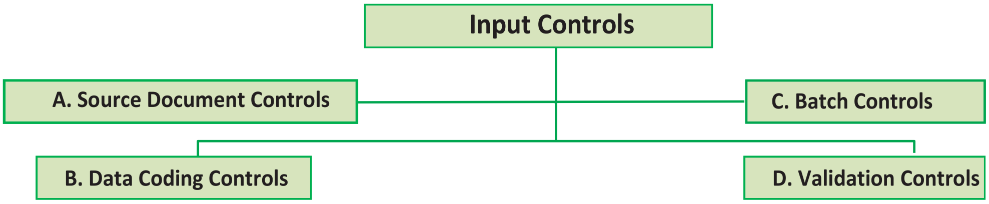


Fig. 3.4.3: Classification of Input Controls

A Source Document Controls: In systems that use physical source documents to initiate transactions, careful control must be exercised over these instruments. Source document fraud can be used to remove assets from the organization. For example, an individual with access to purchase orders and receiving reports could fabricate a purchase transaction to a non-existent supplier. In the absence of other compensating controls to detect this type of fraud, the system would create an account payable and subsequently write a cheque for payment. To control against this type of exposure, the organization must implement control procedures over source documents to account for each document.

B. **Data Coding Controls:** Two types of errors - **Transcription** and **Transposition** errors can corrupt a data code and cause processing errors. Any of these errors can cause serious problems in data processing if they go undetected. These simple errors can severely disrupt operations.

- **Transcription Errors:** It is a special type of data entry error that is commonly made by human operators or by Optical Character Recognition (OCR) programs. Like **Addition errors** (when an extra digit is added to the code); **Truncation Errors** (when a digit is removed from the code) and **Substitution Errors** (replacement of on digit in a code with another).

- **Transposition Errors:** It is a simple error of data entry that occur when two digits that are either individual or part of larger sequence of numbers are reversed (Transpose) when posting a transaction. For example, a sales order for customer 987654 that is transposed into 897654 will be posted to the wrong customer's account. A similar error in an inventory item code on a purchase order could result in ordering unneeded inventory and failing to order inventory that is needed.

C. **Batch Controls:** Batching is the process of grouping together transactions that bear some type of relationship to each other. Various controls can be exercises over the batch to prevent or detect errors or irregularities. To identify errors or irregularities in either a physical or logical batch, three types of control totals are as follows:

- **Financial totals:** Grand totals calculated for each field containing money amounts.

- **Hash totals:** Grand totals calculated for any code on a document in the batch, eg., the source document serial numbers can be totalled.

- **Document/Record Counts:** Grand totals for number of documents in record in batch.

D. **Validation Controls:** Input validation controls are intended to detect errors in the transaction data before the data are processed. Some of these controls include the following:

- **Field interrogation**: It involves programmed procedures that examine the characters of the data in the field. This includes the checks like Limit Check (against predefined limits), Picture Checks (against entry into processing of incorrect/invalid characters), valid check codes (against predetermined transactions codes, tables) etc.
- **Record interrogation**: This includes the reasonableness check (Whether the value specified in a field is reasonable for that particular field?); Valid Sign (to determine which sign is valid for a numeric field) and Sequence Check (to follow a required order matching with logical records.)
- **File Interrogation**: This includes version usage; internal and external labeling; data file security; file updating and maintenance authorization etc.

III. Communication Controls: These discuss exposures in the communication subsystem, controls over physical components, communication line errors, flows, and links, topological controls, channel access controls, controls over subversive attacks, internetworking controls, communication architecture controls, audit trail controls, and existence controls. Some communication controls are as follows:

(a) Physical Component Controls: These controls incorporate features that mitigate the possible effects of exposures.

(b) Line Error Control: Whenever data is transmitted over a communication line, recall that it can be received in error because of attenuation distortion, or noise that occurs on the line. These errors must be detected and corrected.

(c) Flow Controls: Flow controls are needed because two nodes in a network can differ in terms of the rate at which they can send, received, and process data. For example, a main frame can transmit data to a microcomputer terminal.

(d) Link Controls: In Wide Area Network (WAN), line error control and flow control are important functions in the component that manages the link between two nodes in a network.

(e) Channel Access Controls: Two different nodes in a network can compete to use a communication channel. Whenever the possibility of contention for the channel exists, some type of channel access control technique must be used.

IV. Processing Controls

The processing subsystem is responsible for computing, sorting, classifying, and summarizing data. Its major components are the Central Processor in which programs are executed, the real or virtual memory in which program instructions and data are stored, the operating system that manages system resources, and the application programs that execute instructions to achieve specific user requirements. Some of these controls are as follows:

(i) **Processor Controls:** Table 3.4.6 enlists the Controls to reduce expected losses from errors and irregularities associated with Central processors.

Table 3.4.6: Processor Controls

Control	Explanation
Error Detection and Correction	Occasionally, processors might malfunction because of design errors, manufacturing defects, damage, fatigue, electromagnetic interference, and ionizing radiation. The failure might be transient (that disappears after a short period), intermittent (that reoccurs periodically), or permanent (that does not correct with time). For the transient and intermittent errors; retries and re-execution might be successful, whereas for permanent errors, the processor must halt and report error.
Multiple Execution States	It is important to determine the number of and nature of the execution states enforced by the processor. This helps auditors to determine which user processes will be able to carry out unauthorized activities, such as gaining access to sensitive data maintained in memory regions assigned to the operating system or other user processes.
Timing Controls	An operating system might get stuck in an infinite loop. In the absence of any control, the program will retain use of processor and prevent other programs from undertaking their work.
Component Replication	In some cases, processor failure can result in significant losses. Redundant processors allow errors to be detected and corrected. If processor failure is permanent in multicomputer or multiprocessor architectures, the system might reconfigure itself to isolate the failed processor.

(ii) **Real Memory Controls:** This comprises the fixed amount of primary storage in which programs or data must reside for them to be executed or referenced by the central processor. Real memory controls seek to detect and correct errors that occur in memory cells and to protect areas of memory assigned to a program from illegal access by another program.

(iii) **Virtual Memory Controls:** Virtual Memory exists when the addressable storage space is larger than the available real memory space. To achieve this outcome, a control mechanism must be in place that maps virtual memory addresses into real memory addresses.

(iv) **Data Processing Controls:** These perform validation checks to identify errors during processing of data. They are required to ensure both the completeness and the accuracy of data being processed. Normally, the processing controls are enforced through database management system that stores the data. However, adequate controls should be enforced through the front-end application system also to have consistency in the control process.

V. Database Controls

Protecting the integrity of a database when application software acts as an interface to interact between the user and the database, are called **Update Controls** and **Report Controls**.

Major **Update Controls** are as follows:

- **Sequence Check between Transaction and Master Files:** Synchronization and the correct sequence of processing between the master file and transaction file is critical to maintain the integrity of updating, insertion or deletion of records in the master file with respect to the transaction records. If errors, in this stage are overlooked, it leads to corruption of the critical data.
- **Ensure All Records on Files are processed:** While processing, the transaction file records mapped to the respective master file, and the end-of-file of the transaction file with respect to the end-of-file of the master file is to be ensured.
- **Process multiple transactions for a single record in the correct order:** Multiple transactions can occur based on a single master record (e.g. dispatch of a product to different distribution centers). Here, the order in which transactions are processed against the product master record must be done based on a sorted transaction codes.
- **Maintain a suspense account:** When mapping between the master record to transaction record results in a mismatch due to failure in the corresponding record entry in the master record; then these transactions are maintained in a suspense account.

Major **Report Controls** are as follows:

- **Standing Data:** Application programs use many internal tables to perform various functions like gross pay calculation, billing calculation based on a price table, bank interest calculation etc. Maintaining integrity of the pay rate table, price table and interest table is critical within an organization.
- **Print-Run-to Run Control Totals:** Run-to-Run control totals help in identifying errors or irregularities like record dropped erroneously from a transaction file, wrong sequence of updating or the application software processing errors.
- **Print Suspense Account Entries:** Similar to the update controls, the suspense account entries are to be periodically monitors with the respective error file and action taken on time.
- **Existence/Recovery Controls:** The back-up and recovery strategies together encompass the controls required to restore failure in a database. Backup strategies are implemented using prior version and logs of transactions or changes to the database. Recovery strategies involve roll-forward (current state database from a previous version) or the roll-back (previous state database from the current version) methods.

VI. Output Controls

Output Controls ensure that the data delivered to users will be presented, formatted and delivered in a consistent and secured manner. Output can be in any form, it can either be a printed data report or a database file in a removable media. Various Output Controls are as follows:

- **Storage and Logging of sensitive, critical forms:** Pre-printed stationery should be stored securely to prevent unauthorized destruction or removal and usage.
- **Logging of output program executions:** When programs used for output of data are executed, these should be logged and monitored; otherwise confidentiality/integrity of the data may be compromised.
- **Spooling/Queuing:** "Spool" is an acronym for "Simultaneous Peripherals Operations Online". This is a process used to ensure that the user can continue working, while the print operation is getting completed. A queue is the list of documents waiting to be printed on a particular printer; this should not be subject to unauthorized modifications.

- **Controls over printing:** Outputs should be made on the correct printer and it should be ensured that unauthorized disclosure of information printed does not take place.
- **Report Distribution and Collection Controls:** Distribution of reports should be made in a secure way to prevent unauthorized disclosure of data. It should be made immediately after printing to ensure that the time gap between generation and distribution is reduced. A log should be maintained for reports that were generated and to whom these were distributed. Retention Controls: Retention controls consider the duration for which outputs should be retained before being destroyed. Retention control requires that a date should be determined for each output item produced.

3.5 INFORMATION SYSTEMS' AUDITING

IS Auditing is defined as the process of attesting objectives (those of the external auditor) that focus on asset safeguarding, data integrity and management objectives (those of the internal auditor) that include effectiveness and efficiency both. This enables organizations to better achieve four major objectives (Fig. 3.5.1) that are as follows:

a. **Asset Safeguarding Objectives:** The information system assets (hardware, software, data information etc.) must be protected by a system of internal controls from unauthorized access.

b. **Data Integrity Objectives:** It is a fundamental attribute of IS Auditing. The importance to maintain integrity of data of an organization requires all the time. It is also important from the business perspective of the decision maker, competition and the market environment.

c. **System Effectiveness Objectives:** Effectiveness of a system is evaluated by auditing the characteristics and objective of the system to meet business and user requirements.

d. **System Efficiency Objectives:** To optimize the use of various information system resources (machine time, peripherals, system software and labour) along with the impact on its computing environment.

3.5.1 Need for Audit of Information Systems

Factors influencing an organization toward controls and audit of computers and the impact of the information systems audit function on organizations are depicted in the Fig. 3.5.1.

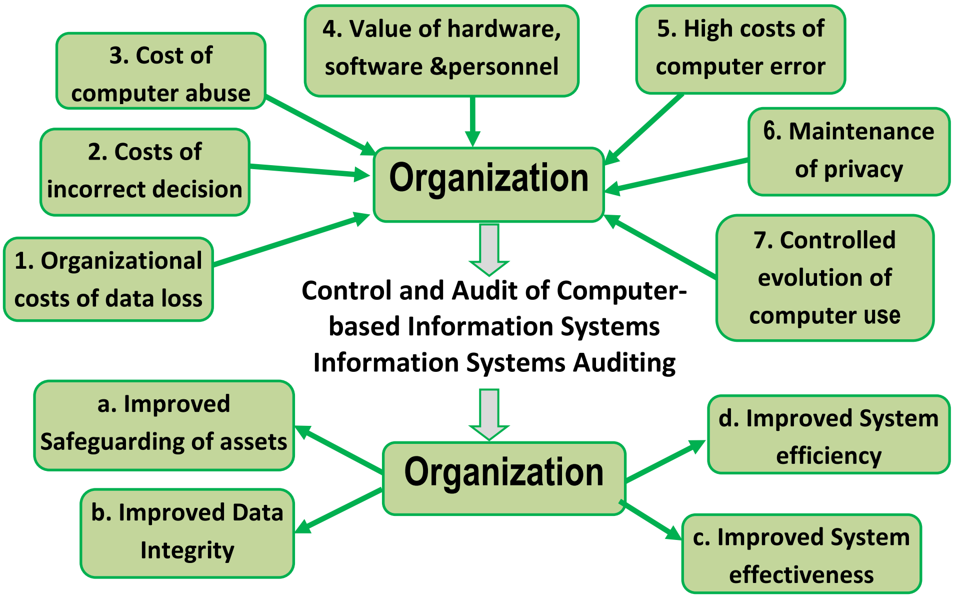

3. Cost of computer abuse
4. Value of hardware, software &personnel
5. High costs of computer error
2. Costs of incorrect decision
Organization
6. Maintenance of privacy
1. Organizational costs of data loss
7. Controlled evolution of computer use
Control and Audit of Computer-based Information Systems Information Systems Auditing
a. Improved Safeguarding of assets
d. Improved System efficiency
Organization
b. Improved Data Integrity
c. Improved System effectiveness

Fig. 3.5.1: Impact of Controls and Audit influencing an Organization

Let us now discuss these reasons in detail:

1. **Organizational Costs of Data Loss:** Data is a critical resource of an organization for its present and future process and its ability to adapt and survive in a changing environment.

2. **Cost of Incorrect Decision Making:** Management and operational controls taken by managers involve detection, investigations and correction of the processes. These high-level decisions require accurate data to make quality decision rules.

3. **Costs of Computer Abuse:** Unauthorized access to computer systems, malwares, unauthorized physical access to computer facilities and unauthorized copies of sensitive data can lead to destruction of assets (hardware, software, data, information etc.)

4. **Value of Computer Hardware, Software and Personnel:** These are critical resources of an organization, which has a credible impact on its infrastructure and business competitiveness.

5. **High Costs of Computer Error:** In a computerized enterprise environment where many critical business processes are performed, a data error during entry or process would cause great damage.

6. **Maintenance of Privacy:** Today, data collected in a business process contains private information about an individual too. These data were also

collected before computers but now, there is a fear that privacy has eroded beyond acceptable levels.

7. **Controlled evolution of computer Use:** Use of Technology and reliability of complex computer systems cannot be guaranteed and the consequences of using unreliable systems can be destructive.

3.5.2 Tools for IS Audit

Today, organizations produce information on a real-time, online basis. Real-time recordings need real-time auditing to provide continuous assurance about the quality of the data that is continuous auditing. Continuous auditing enables auditors to significantly reduce and perhaps to eliminate the time between occurrence of the client's events and the auditor's assurance services thereon. Errors in a computerized system are generated at high speeds and the cost to correct and rerun programs are high. If these errors can be detected and corrected at the point or closest to the point of their occurrence the impact thereof would be the least. Continuous auditing techniques use two bases for collecting audit evidence. One is the use of embedded modules in the system to collect, process, and print audit evidence and the other is special audit records used to store the audit evidence collected.

Types of Audit Tools: Different types of continuous audit techniques may be used. Some modules for obtaining data, audit trails and evidences may be built into the programs. Audit software is available, which could be used for selecting and testing data. Many audit tools are also available; some of them are described below:

(i) **Snapshots:** Tracing a transaction is a computerized system can be performed with the help of snapshots or extended records. The snapshot software is built into the system at those points where material processing occurs which takes images of the flow of any transaction as it moves through the application. These images can be utilized to assess the authenticity, accuracy, and completeness of the processing carried out on the transaction. The main areas to dwell upon while involving such a system are to locate the snapshot points based on materiality of transactions when the snapshot will be captured and the reporting system design and implementation to present data in a meaningful way.

(ii) **Integrated Test Facility (ITF):** The ITF technique involves the creation of a dummy entity in the application system files and the processing of audit test data against the entity as a means of verifying processing authenticity, accuracy, and completeness. This test data would be included with the normal production data used as input to the application system. In such cases the auditor must decide what would be the method to be used to enter test data and the methodology for removal of the effects of the ITF transactions.

(iii) System Control Audit Review File (SCARF): The SCARF technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. The information collected is written onto a special audit file- the SCARF master files. Auditors then examine the information contained on this file to see if some aspect of the application system needs follow-up. In many ways, the SCARF technique is like the snapshot technique along with other data collection capabilities.

(iv) Continuous and Intermittent Simulation (CIS): This is a variation of the SCARF continuous audit technique. This technique can be used to trap exceptions whenever the application system uses a database management system. During application system processing, CIS executes in the following way:

- The database management system reads an application system transaction. It is passed to CIS. CIS then determines whether it wants to examine the transaction further. If yes, the next steps are performed or otherwise it waits to receive further data from the database management system.
- CIS replicates or simulates the application system processing.
- Every update to the database that arises from processing the selected transaction will be checked by CIS to determine whether discrepancies exist between the results it produces and those the application system produces.
- Exceptions identified by CIS are written to an exception log file.
- The advantage of CIS is that it does not require modifications to the application system and yet provides an online auditing capability.

(v) Audit Hooks: There are audit routines that flag suspicious transactions. For example, internal auditors at Insurance Company determined that their policyholder system was vulnerable to fraud every time a policyholder changed his or her name or address and then subsequently withdrew funds from the policy. They devised a system of audit hooks to tag records with a name or address change. The internal audit department will investigate these tagged records for detecting fraud. When audit hooks are employed, auditors can be informed of questionable transactions as soon as they occur. This approach of real-time notification displays a message on the auditor's terminal.

3.6 AUDIT TRAIL

Audit Trails are logs that can be designed to record activity at the system, application, and user level. When properly implemented, audit trails provide an important detective control to help accomplish security policy objectives. Many operating systems allow management to select the level of auditing to be provided by the system. This determines 'which events will be recorded in the log'. An effective audit policy will capture all significant events without cluttering the log with trivial activity.

Audit trail controls attempt to ensure that a chronological record of all events that have occurred in a system is maintained. This record is needed to answer queries, fulfill statutory requirements, detect the consequences of error and allow system monitoring and tuning.

- The **Accounting Audit Trail** shows the source and nature of data and processes that update the database.
- The **Operations Audit Trail** maintains a record of attempted or actual resource consumption within a system.

Applications System Controls involve ensuring that individual application systems safeguard assets (reducing expected losses), maintain data integrity (ensuring complete, accurate and authorized data) and achieve objectives effectively and efficiently from the perspective of users of the system from within and outside the organization.

(i) Audit Trail Objectives: Audit trails can be used to support security objectives in three ways:

- **Detecting Unauthorized Access:** Detecting unauthorized access can occur in real time or after the fact. The primary objective of real-time detection is to protect the system from outsiders who are attempting to breach system controls. A real-time audit trail can also be used to report on changes in system performance that may indicate infestation by a virus or worm. Depending upon how much activity is being logged and reviewed; real-time detection can impose a significant overhead on the operating system, which can degrade operational performance. After-the-fact detection logs can be stored electronically and reviewed periodically or as needed. When properly designed, they can be used to determine if unauthorized access was accomplished, or attempted and failed.

- **Reconstructing Events:** Audit analysis can be used to reconstruct the steps that led to events such as system failures, security violations by individuals, or application processing errors. Knowledge of the conditions that existed at the time of a system failure can be used to assign responsibility and to avoid similar situations in the future. Audit trail analysis also plays an important role in accounting control. For example, by maintaining a record of all changes to account balances, the audit trail can be used to reconstruct accounting data files that were corrupted by a system failure.
- **Personal Accountability:** Audit trails can be used to monitor user activity at the lowest level of detail. This capability is a preventive control that can be used to influence behavior. Individuals are likely to violate an organization's security policy if they know that their actions are not recorded in an audit log.

(ii) Implementing an Audit Trail: The information contained in audit logs is useful to accountants in measuring the potential damage and financial loss associated with application errors, abuse of authority, or unauthorized access by outside intruders. Logs also provide valuable evidence or assessing both the adequacies of controls in place and the need for additional controls. Audit logs, however, can generate data in overwhelming detail. Important information can easily get lost among the superfluous detail of daily operation. Thus, poorly designed logs can be dysfunctional.

3.6.1 Auditing Environmental Controls

Related aspects are given as follows:

(a) Role of Auditor in Auditing Environmental Controls: The attack on the World Trade Centre in 2001 has created a worldwide alert bringing focus on business continuity planning and environmental controls. Audit of environmental controls should form a critical part of every IS audit plan. The IS auditor should satisfy not only the effectiveness of various technical controls but also the overall controls safeguarding the business against environmental risks. Some of the critical audit considerations that an IS auditor should consider while conducting his/her audit is given below:

(b) Audit of Environmental Controls: Audit of environmental controls requires the IS auditor to conduct physical inspections and observe practices. Auditing environmental controls requires knowledge of building mechanical and electrical systems as well as fire codes. The IS auditor needs to be able to determine if such controls are effective and if they are cost-effective. Auditing environmental controls requires attention to these and other factors and activities, including:

- **Power conditioning:** The IS auditor should determine how frequently power conditioning equipment, such as UPS, line conditioners, surge protectors, or motor generators, are used, inspected and maintained and if this is performed by qualified personnel.
- **Backup power:** The IS auditor should determine if backup power is available via electric generators or UPS and how frequently they are tested. S/he should examine maintenance records to see how frequently these components are maintained and if this is done by qualified personnel.
- **Heating, Ventilation, and Air Conditioning (HVAC):** The IS auditor should determine if HVAC systems are providing adequate temperature and humidity levels, and if they are monitored. Also, the auditor should determine if HVAC systems are properly maintained and if qualified persons do this.
- **Water detection:** The IS auditor should determine if any water detectors are used in rooms where computers are used. He or she should determine how frequently these are tested and if they are monitored.
- **Fire detection and suppression:** The IS auditor should determine if fire detection equipment is adequate, if staff members understand their function, and if they are tested. He or she should determine how frequently fire suppression systems are inspected and tested, and if the organization has emergency evacuation plans and conducts fire drills.
- **Cleanliness:** The IS auditor should examine data centers to see how clean they are. IT equipment air filters and the inside of some IT components should be examined to see if there is an accumulation of dust and dirt.

3.6.2 Auditing Physical Security Controls

(a) **Role of IS Auditor in Auditing Physical Access Controls:** Auditing physical access requires the auditor to review the physical access risk and controls to form an opinion on the effectiveness of the physical access controls. This involves the following:

- **Risk Assessment:** The auditor must satisfy him/herself that the risk assessment procedure adequately covers periodic and timely assessment of all assets, physical access threats, vulnerabilities of safeguards and exposures there from.
- **Controls Assessment:** The auditor based on the risk profile evaluates whether the physical access controls are in place and adequate to protect the IS assets against the risks.
- **Review of Documents:** It requires examination of relevant documentation such as the security policy and procedures, premises plans, building plans, inventory list and cabling diagrams.

(b) Audit of Physical Access Controls: Auditing physical security controls requires knowledge of natural and manmade hazards, physical security controls, and access control systems.

(i) Siting and Marking: Auditing building siting and marking requires attention to several key factors and features, including:

- o **Proximity to hazards:** The IS auditor should estimate the building's distance to natural and manmade hazards, such as Dams; Rivers, lakes, and canals; Natural gas and petroleum pipelines; Water mains and pipelines; Earthquake faults; Areas prone to landslides; Volcanoes; Severe weather such as hurricanes, cyclones, and tornadoes; Flood zones; Military bases; Airports; Railroads and Freeways. The IS auditor should determine if any risk assessment regarding hazards has been performed and if any compensating controls that were recommended have been carried out.
- o **Marking:** The IS auditor should inspect the building and surrounding area to see if building(s) containing information processing equipment identify the organization. Marking may be visible on the building itself, but also on signs or parking stickers on vehicles.

(ii) Physical barriers: This includes fencing, walls, barbed/razor wire, bollards, and crash gates. The IS auditor needs to understand how these are used to control access to the facility and determine their effectiveness.

(iii) Surveillance: The IS auditor needs to understand how video and human surveillance are used to control and monitor access. He or she needs to understand how (and if) video is recorded and reviewed, and if it is effective in preventing or detecting incidents.

(iv) Guards and dogs: The IS auditor needs to understand the use and effectiveness of security guards and guard dogs. Processes, policies, procedures, and records should be examined to understand required activities and how they are carried out.

(v) Key-Card systems: The IS auditor needs to understand how key-card systems are used to control access to the facility. Some points to consider include: Work zones: Whether the facility is divided into security zones and which persons are permitted to access which zones whether key-card systems record personnel movement; What processes and procedures are used to issue key-cards to employees? etc.

3.6.3 Auditing Logical Access Controls

(a) Role of IS Auditor in Auditing Logical Access Controls

Auditing Logical Access Controls requires attention to several key areas that include the following:

(i) Network Access Paths: The IS auditor should conduct an independent review of the IT infrastructure to map out the organization's logical access paths. This will require considerable effort and may require the use of investigative and technical tools, as well as specialized experts on IT network architecture.

(ii) Documentation: The IS auditor should request network architecture and access documentation to compare what was discovered independently against existing documentation. The auditor will need to determine why any discrepancies exist. Similar investigations should take place for each application to determine all of the documented and undocumented access paths to functions and data.

(b) Audit of Logical Access Controls

(I) User Access Controls: User access controls are often the only barrier between unauthorized parties and sensitive or valuable information. This makes the audit of user access controls particularly significant. Auditing user access controls requires keen attention to several key factors and activities in four areas:

(i) **Auditing User Access Controls:** These are to determine if the controls themselves work as designed. Auditing user access controls requires attention to several factors, including:

- **Authentication:** The auditor should examine network and system resources to determine if they require authentication, or whether any resources can be accessed without first authenticating.
- **Access violations:** The auditor should determine if systems, networks, and authentication mechanisms can log access violations. These usually exist in the form of system logs showing invalid login attempts, which may indicate intruders who are trying to log in to employee user accounts.
- **User account lockout:** The auditor should determine if systems and networks can automatically lock user accounts that are the target of attacks. A typical system configuration is one that will lock a user account after five unsuccessful logins attempts within a short period.
- **Intrusion detection and prevention:** The auditor should determine if there are any IDSs or IPSs that would detect authentication-bypass attempts. The auditor should examine these systems to see whether they have up-to-date configurations and signatures, whether they generate alerts, and whether the recipients of alerts act upon them.
- **Dormant accounts:** The IS auditor should determine if any automated or manual process exists to identify and close dormant accounts. Dormant accounts are user (or system) accounts that exist but are unused. These accounts represent a risk to the environment, as they represent an additional path between intruders and valuable or sensitive data.
- **Shared accounts:** The IS auditor should determine if there are any shared user accounts; these are user accounts that are routinely (or even infrequently) used by more than one person. The principal risk with shared accounts is the inability to determine accountability for actions performed with the account.
- **System accounts:** The IS auditor should identify all system-level accounts on networks, systems, and applications. The purpose of each system account should be identified, and it should be determined if each system account is still required (some may be artefacts of the initial implementation or of an upgrade or migration). The IS auditor should

determine who has the password for each system account, whether accesses by system accounts are logged, and who monitors those logs.

(ii) **Auditing Password Management:** The IS auditor needs to examine password configuration settings on information systems to determine how passwords are controlled. Some of the areas requiring examination are- how many characters must a password have and whether there is a maximum length; how frequently must passwords be changed; whether former passwords may be used again; whether the password is displayed when logging in or when creating a new password etc.

(iii) **Auditing User Access Provisioning:** Auditing the user access provisioning process requires attention to several key activities, including:

- ♦ **Access request processes:** The IS auditor should identify all user access request processes and determine if these processes are used consistently throughout the organization.
- ♦ **Access approvals:** The IS auditor needs to determine how requests are approved and by what authority they are approved. The auditor should determine if system or data owners approve access requests, or if any accesses are ever denied.
- ♦ **New employee provisioning:** The IS auditor should examine the new employee provisioning process to see how a new employee's user accounts are initially set up. The auditor should determine if new employees' managers are aware of the access requests that their employees are given and if they are excessive.
- ♦ **Segregation of Duties (SOD):** The IS auditor should determine if the organization makes any effort to identify segregation of duties. This may include whether there are any SOD matrices in existence and if they are actively used to make user access request decisions.
- ♦ **Access reviews:** The IS auditor should determine if there are any periodic access reviews and what aspects of user accounts are reviewed; this may include termination reviews, internal transfer reviews, SOD reviews, and dormant account reviews.

(iv) **Auditing Employee Terminations:** Auditing employee terminations requires attention to several key factors, including:

- **Termination process:** The IS auditor should examine the employee termination process and determine its effectiveness. This examination should include understanding on how terminations are performed and how user account management personnel are notified of terminations.
- **Access reviews:** The IS auditor should determine if any internal reviews of terminated accounts are performed, which would indicate a pattern of concern for effectiveness in this important activity. If such reviews are performed, the auditor should determine if any missed terminations are identified and if any process improvements are undertaken.
- **Contractor access and terminations:** The IS auditor needs to determine how contractor access and termination is managed and if such management is effective.

(II) User Access Logs: The IS auditor needs to determine what events are recorded in access logs. The IS auditor needs to understand the capabilities of the system being audited and determine if the right events are being logged, or if logging is suppressed on events that should be logged.

- **Centralized access logs:** The IS auditor should determine if the organization's access logs are aggregated or if they are stored on individual systems.
- **Access log protection:** The auditor needs to determine if access logs can be altered, destroyed, or attacked to cause the system to stop logging events. For especially high-value and high-sensitivity environments, the IS auditor needs to determine if logs should be written to digital media that is unalterable, such as optical WORM (write once read many) media.
- **Access log review:** The IS auditor needs to determine if there are policies, processes, or procedures regarding access log review. The auditor should determine if access log reviews take place, who performs them, how issues requiring attention are identified, and what actions are taken when necessary.
- **Access log retention:** The IS auditor should determine how long access logs are retained by the organization and if they are back up.

(III) Investigative Procedures: Auditing investigative procedures requires attention to several key activities, including:

- **Investigation policies and procedures:** The IS auditor should determine if there are any policies or procedures regarding security investigations. This would include who is responsible for performing investigations, where information about investigations is stored, and to whom the results of investigations are reported.
- **Computer crime investigations:** The IS auditor should determine if there are policies, processes, procedures, and records regarding computer crime investigations. The IS auditor should understand how internal investigations are transitioned to law enforcement.
- **Computer forensics:** The IS auditor should determine if there are procedures for conducting computer forensics. The auditor should also identify tools and techniques that are available to the organization for the acquisition and custody of forensic data. The auditor should identify whether any employees in the organization have received computer forensics training and are qualified to perform forensic investigations.

(IV) Internet Points of Presence: The IS auditor who is performing a comprehensive audit of an organization's system and network system needs to perform a "points of presence" audit to discover what technical information is available about the organization's Internet presence. Some of the aspects of this intelligence gathering include:

- **Search engines:** Google, Yahoo!, and other search engines should be consulted to see what information about the organization is available. Searches should include the names of company officers and management, key technologists, and any internal-only nomenclature such as the names of projects.
- **Social networking sites:** Social networking sites such as Facebook, LinkedIn, Myspace, and Twitter should be searched to see what employees, former employees, and others are saying about the organization. Any authorized or unauthorized "fan pages" should be searched as well.
- **Online sales sites:** Sites such as Craigslist and eBay should be searched to see if anything related to the organization is sold online.
- **Domain names:** The IS auditor should verify contact information for known domain names, as well as related domain names. For instance, for the organization mycompany.com; organizations should search for domain names such as mycompany.net, mycompany.info, and

mycompany.biz to see if they are registered and what contents are available.

- **Justification of Online Presence:** The IS auditor should examine business records to determine on what basis the organization established online capabilities such as e-mail, Internet-facing web sites, Internet e-commerce, Internet access for employees, and so on. These services add risk to the business and consume resources. The auditor should determine if a viable business case exists to support these services or if they exist as a "benefit" for employees.

3.6.4 Managerial Controls and their Audit Trails

The auditors play a vital role in evaluating the performance of various controls under managerial controls. Some of the key areas that auditors should pay attention to while evaluating Managerial controls and its types are provided below:

I. Top Management and Information Systems Management Controls

The major activities that senior management must perform are – **Planning, Organizing, Leading** and **Controlling**. The Role of auditor at each activity is discussed below:

- **Planning:** Auditors need to evaluate whether top management has formulated a high-quality information system's plan that is appropriate to the needs of an organization or not. A poor-quality information system is ineffective and inefficient leading to losing of its competitive position within the marketplace.

- **Organizing:** Auditors should be concerned about how well top management acquires and manages staff resources.

- **Leading:** Generally, the auditors examine variables that often indicate when motivation problems exist or suggest poor leadership – for example, staff turnover statistics, frequent failure of projects to meet their budget and absenteeism level to evaluate the leading function. Auditors may use both formal and informal sources of evidence to evaluate how well top managers communicate with their staff.

- **Controlling:** Auditors should focus on subset of the control activities that should be performed by top management – namely, those aimed at ensuring that the information systems function accomplishes its objectives at a global level. Auditors must evaluate whether top management's choice to the means of control over the users of IS services is likely to be effective or not.

II. System Development Management Controls

Three different types of audits may be conducted during system development process as discussed in the Table 3.6.1:

Table 3.6.1: Different types of Audit during System Development Process

Concurrent Audit	Auditors are members of the system development team. They assist the team in improving the quality of systems development for the specific system they are building and implementing.
Post - implementation Audit	Auditors seek to help an organization learn from its experiences in the development of a specific application system. In addition, they might be evaluating whether the system needs to be scrapped, continued, or modified in some way.
General Audit	Auditors evaluate systems development controls overall. They seek to determine whether they can reduce the extent of substantive testing needed to form an audit opinion about management's assertions relating to the financial statements for systems effectiveness and efficiency.

An external auditor is more likely to undertake general audits rather than concurrent or post-implementation audits of the systems development process. For internal auditors, management might require that they participate in the development of material application systems or undertake post-implementation reviews of material application systems as a matter of course.

III. Programming Management Controls

Some of the major concerns that an Auditor should address under different activities involved in Programming Management Control Phase are provided in Table 3.6.2.

Table 3.6.2: Audit Trails under Programming Management Controls

Phase	Audit Trails
Planning	♦ They should evaluate whether nature of and extent of planning are appropriate to different types of s/w that are developed or acquired. ♦ They must evaluate how well the planning work is being undertaken.
Control	♦ They must evaluate whether the nature of an extent of control activities undertaken are appropriate for the different types of software that are developed or acquired. ♦ They must gather evidence on whether the control procedures are operating reliably. For example - they might first choose a sample if past and current software development and acquisition projects carried

	out at different locations in the organization they are auditing.
Design	♦ Auditors should find out whether programmers use some type of systematic approach to design. ♦ Auditors can obtain evidence of the design practices used by undertaking interviews, observations, and reviews of documentation.
Coding	♦ Auditors should seek evidence – • On the level of care exercised by programming management in choosing a module implementation and integration strategy. • To determine whether programming management ensures that programmers follow structured programming conventions. • To check whether programmers employ automated facilities to assist them with their coding work.
Testing	♦ Auditors can use interviews, observations, and examination of documentation to evaluate how well unit testing is conducted. ♦ Auditors are most likely concerned primarily with the quality of integration testing work carried out by information systems professionals rather than end users. ♦ Auditors primary concern is to see that whole-of-program tests have been undertaken for all material programs and that these tests have been well-designed and executed.
Operation and Main-tenance	♦ Auditors need to ensure effectively and timely reporting of maintenance needs that occur so that maintenance is carried out in a well-controlled manner. ♦ Auditors should ensure that management has implemented a review system and assigned responsibility for monitoring the status of operational programs.

IV. Data Resource Management Controls

- ♦ Auditors should determine what controls are exercised to maintain data integrity. They might also interview database users to determine their level of awareness of these controls.

- ♦ Auditors might employ test data to evaluate whether access controls and update controls are working.

V. Quality Assurance Management Controls

- Auditors might use interviews, observations and reviews of documentation to evaluate how well Quality Assurance (QA) personnel perform their monitoring role.
- Auditors might evaluate how well QA personnel make recommendations for improved standards or processes through interviews, observations, and reviews of documentation.
- Auditors can evaluate how well QA personnel undertake the reporting function and training through interviews, observations, and reviews of documentation.

VI. Security Management Controls

- Auditors must evaluate whether security administrators are conducting ongoing, high-quality security reviews or not;
- Auditors check whether the organizations audited have appropriate, high-quality disaster recovery plan in place; and
- Auditors check whether the organizations have opted for an appropriate insurance plan or not.

VII. Operations Management Controls

- Auditors should pay concern to see whether the documentation is maintained securely and that it is issued only to authorized personnel.
- Auditors can use interviews, observations, and review of documentation to evaluate -
  - the activities of documentation librarians;
  - how well operations management undertakes the capacity planning ad performance monitoring function;
  - the reliability of outsourcing vendor controls;
  - whether operations management is monitoring compliance with the outsourcing contract; and
  - Whether operations management regularly assesses the financial viability of any outsourcing vendors that an organization uses.

3.6.5 Application Controls and their Audit Trails

Audit Trail Controls: Two types of audit trails that should exist in each subsystem are as follows:

- An **Accounting Audit Trail** to maintain a record of events within the subsystem; and
- An **Operations Audit Trail** to maintain a record of the resource consumption associated with each event in the subsystem.

We shall now discuss Audit Trails for Application Controls in detail.

I. Boundary Controls

This maintains the chronology of events that occur when a user attempts to gain access to and employ systems resources. This includes the following:

- Identity of the would-be user of the system;
- Authentication information supplied;
- Resources requested;
- Action privileges requested;
- Terminal Identifier;
- Start and Finish Time;
- Number of Sign-on attempts;
- Resources provided/denied; and

Accounting Audit Trail

- Action privileges allowed/denied.

Operations Audit Trail

- Resource usage from log-on to log-out time.
- Log of Resource consumption.

II. Input Controls

This maintains the chronology of events from the time data and instructions are captured and entered into an application system until the time they are deemed valid and passed onto other subsystems within the application system.

Accounting Audit Trail

- The identity of the person(organization) who was the source of the data;
- The identity of the person(organization) who entered the data into the system;
- The time and date when the data was captured;
- The identifier of the physical device used to enter the data into the system;
- The account or record to be updated by the transaction;
- The standing data to be updated by the transaction;
- The details of the transaction; and
- The number of the physical or logical batch to which the transaction belongs.

Operations Audit Trail

- Time to key in a source document or an instrument at a terminal;
- Number of read errors made by an optical scanning device;
- Number of keying errors identified during verification;
- Frequency with which an instruction in a command language is used; and
- Time taken to invoke an instruction using a light pen versus a mouse.

III. Communication Controls

This maintains a chronology of the events from the time a sender dispatches a message to the time a receiver obtains the message.

Accounting Audit Trail

- Unique identifier of the source/sink node;
- Unique identifier of each node in the network that traverses the message; Unique identifier of the person or process authorizing dispatch of the message; Time and date at which the message was dispatched;
- Time and date at which the message was received by the sink node;
- Time and date at which node in the network was traversed by the message; and
- Message sequence number; and the image of the message received at each node traversed in the network.

Operations Audit Trail

- Number of messages that have traversed each link and each node;

- Queue lengths at each node; Number of errors occurring on each link or at each node; Number of retransmissions that have occurred across each link; Log of errors to identify locations and patterns of errors;
- Log of system restarts; and
- Message transit times between nodes and at nodes.

IV. Processing Controls

The audit trail maintains the chronology of events from the time data is received from the input or communication subsystem to the time data is dispatched to the database, communication, or output subsystems.

Accounting Audit Trail

- To trace and replicate the processing performed on a data item.
- To follow triggered transactions from end to end by monitoring input data entry, intermediate results and output data values.
- To check for existence of any data flow diagrams or flowcharts that describe data flow in the transaction, and whether such diagrams or flowcharts correctly identify the flow of data.
- To check whether audit log entries recorded the changes made in the data items at any time including who made them.

Operations Audit Trail

- A comprehensive log on hardware consumption – CPU time used, secondary storage space used, and communication facilities used.
- A comprehensive log on software consumption – compilers used, subroutine libraries used, file management facilities used, and communication software used.

V. Database Controls

The audit trail maintains the chronology of events that occur either to the database definition or the database itself.

Accounting Audit Trail

- To confirm whether an application properly accepts, processes, and stores information.
- To attach a unique time stamp to all transactions.

- To attach before-images and after-images of the data item on which a transaction is applied to the audit trail.
- Any modifications or corrections to audit trail transactions accommodating the changes that occur within an application system.
- To not only test the stated input, calculation, and output rules for data integrity, but also should assess the efficacy of the rules themselves.

Operations Audit Trail

- To maintain a chronology of resource consumption events that affects the database definition or the database.

VI. Output Controls

The audit trail maintains the chronology of events that occur from the time the content of the output is determined until the time users complete their disposal of output because it no longer should be retained.

Accounting Audit Trail

- What output was presented to users;
- Who received the output;
- When the output was received; and
- What actions were taken with the output?

Operations Audit Trail

- To maintain the record of resources consumed – graphs, images, report pages, printing time and display rate to produce the various outputs.

3.7 ORGANIZATION STRUCTURE AND RESPONSIBILITIES

Organizations require structure to distribute responsibility to groups of people with specific skills and knowledge. The structure of an organization is called an **Organization Chart** (org chart). Organizing and maintaining an organization structure requires that many factors be considered. In most organizations, the organization chart is a living structure that changes frequently, based upon several conditions including the following:

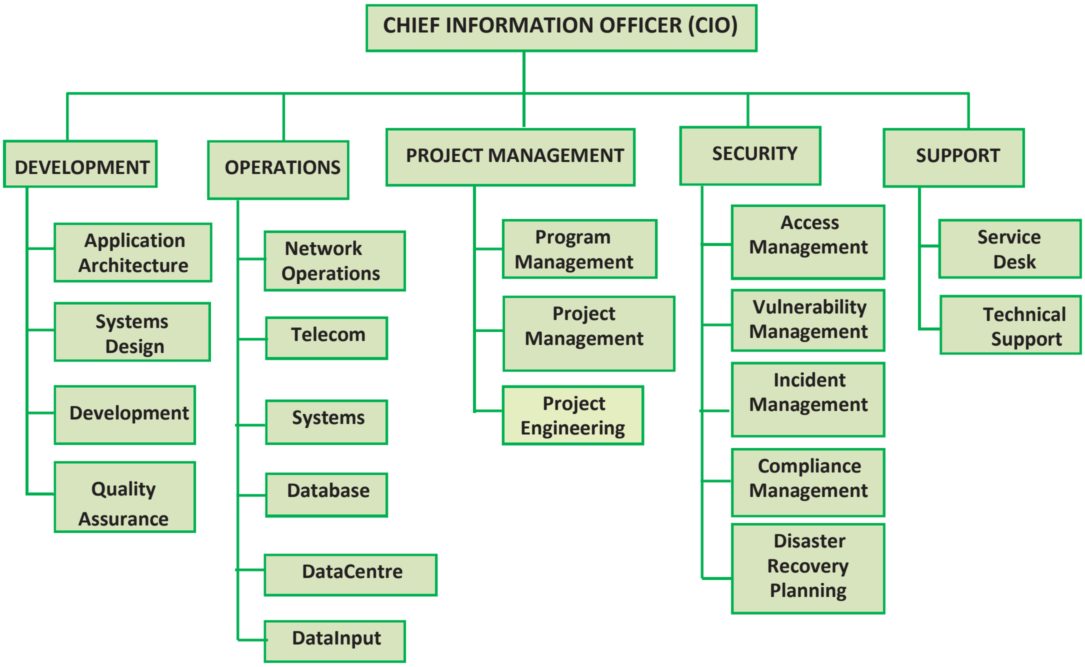


Fig. 3.7.1: Organization Structure - Example

Short and long-term objectives: Organizations sometimes move departments from one executive to another so that departments that were once far from each other (in terms of the org chart structure) will be near each other. This provides new opportunities for developing synergies and partnerships that did not exist before the reorganization (reorg). These organizational changes are usually performed to help an organization meet new objectives that require new partnerships and teamwork that were less important before. Fig. 3.7.1 depicts an organization structure (illustrative only).

- **Market conditions:** Changes in market positions can cause an organization to realign its internal structure to strengthen itself. For example, if a competitor lowers its prices based on a new sourcing strategy, an organization may need to respond by changing its organizational structure to put experienced executives in-charge of specific activities.
- **Regulation:** New regulations may induce an organization to change its organizational structure. For instance, an organization that becomes highly regulated may elect to move its security and compliance group away from IT and place it under the legal department, since compliance has much more to do with legal compliance than industry standards.

- **Available talent:** When someone leaves the organization (or moves to another position within the organization), particularly in positions of leadership, a space opens in the org chart that often cannot be filled right away. Instead, senior management will temporarily change the structure of the organization by moving the leaderless department under the control of someone else. Often, the decisions of how to change the organization will depend upon the talent and experience of existing leaders, in addition to each leader's workload and other factors. For example, if the director of IT program management leaves the organization, the existing department could temporarily be placed under the IT operations department, in this case because the director of IT operations used to run IT program management. Senior management can see how that arrangement works out and later decide whether to replace the director of IT program management position or to do something else.

3.7.1 Roles and Responsibilities

The topic of roles and responsibilities is multidimensional: it encompasses positions and relationships on the organization chart, it defines specific job titles and duties, and it denotes generic expectations and responsibilities regarding the use and protection of assets.

3.7.2 Individual Roles and Responsibilities

Several roles and responsibilities fall upon all individuals throughout the organization.

- **Executive management:** The most senior managers and executives in an organization are responsible for developing the organization's mission, objectives, and goals, as well as policy. Executives are responsible for enacting security policy, which defines (among other things) the protection of assets.

- **Owner:** An owner is an individual (usually but not necessarily a manager) who is the designated owner-steward of an asset. Depending upon the organization's security policy, an owner may be responsible for the maintenance and integrity of the asset, as well as for deciding who is permitted to access the asset. If the asset is information, the owner may be responsible for determining who may access and make changes to the information.

- **Manager:** A manager is, in the general sense, responsible for obtaining policies and procedures and making them available to their staff members. They should also, to some extent, be responsible for their staff members' behaviour.

- **User:** Users are individuals (at any level of the organization) who use assets in the performance of their job duties. Each user is responsible for how he or she uses the asset, and does not permit others to access the asset in his or her name. Users are responsible for performing their duties lawfully and for conforming to organization policies.

These generic roles and responsibilities should apply across the organization chart to include every person in the organization.

3.7.3 Job Titles and Job Descriptions

A Job Title is a label that is assigned to a job description. It denotes a position in the organization that has a given set of responsibilities, and which requires a certain level and focus of education and prior experience.

An organization that has a program of career advancement may have a set of career paths or career ladders that are models showing how employees may advance. For each job title, a career path will show the possible avenues of advancement to other job titles, and the experience required to reach those other job titles.

Job titles in IT have matured and are quite consistent across organizations. This consistency helps organizations in several ways:

- **Recruiting:** When the organization needs to find someone to fill an open position, the use of standard job titles will help prospective candidates more easily find positions that match their criteria.
- **Compensation base lining:** Because of the chronic shortage of talented IT workers, organizations are forced to be more competitive when trying to attract new workers. To remain competitive, many organizations periodically undertake a regional compensation analysis to better understand the levels of compensation paid to IT workers in other organizations. The use of standard job titles makes the task of comparing compensation far easier.
- **Career advancement:** When an organization uses job titles that are consistent in the industry, IT workers have a better understanding of the functions of positions within their own organizations and can more easily plan how they can advance. The remainder of this section includes many IT job titles with a short description (not a full job description by any measure) of the function of that position.

Virtually all organizations also include titles that denote the level of experience, leadership, or span of control in an organization. These titles may include executive vice president, senior vice president, vice president, senior director, director, general manager, senior manager, manager and supervisor. Larger organizations will use more of these, and possibly additional titles such as district manager, group manager, or area manager.

(a) Executive Management: Executive managers are the chief leaders and policymakers in an organization. They set objectives and work directly with the organization's most senior management to help make decisions affecting the future strategy of the organization.

- **CIO (Chief Information Officer):** This is the title of the top most leaders in a larger IT organization.
- **CTO (Chief Technical Officer):** This position is usually responsible for an organization's overall technology strategy. Depending upon the purpose of the organization, this position may be separate from IT.
- **CSO (Chief Security Officer):** This position is responsible for all aspects of security, including information security, physical security, and possibly executive protection (protecting the safety of senior executives).
- **CISO (Chief Information Security Officer):** This position is responsible for all aspects of data-related security. This usually includes incident management, disaster recovery, vulnerability management, and compliance.
- **CPO (Chief Privacy Officer):** This position is responsible for the protection and use of personal information. This position is found in organizations that collect and store sensitive information for large numbers of persons.

(b) Software Development: Positions in software development are involved in the design, development, and testing of software applications.

- **Systems Architect:** This position is usually responsible for the overall information systems architecture in the organization. This may or may not include overall data architecture as well as interfaces to external organizations.
- **Systems Analyst:** A systems analyst is involved with the design of applications, including changes in an application's original design. This position may develop technical requirements, program design, and software test plans. In cases where organizations license applications developed by other companies, systems analysts design interfaces to other applications.

- **Software Developer and Programmer:** This position develops application software. Depending upon the level of experience, persons in this position may also design programs or applications. In organizations that utilize purchased application software, developers often create custom interfaces, application customizations, and custom reports.
- **Software Tester:** This position tests changes in programs made by software developers.

(c) Data Management: Positions in data management are responsible for developing and implementing database designs and for maintaining databases.

- **Database Architect:** This position develops logical and physical designs of data models for applications. With sufficient experience, this person may also design an organization's overall data architecture.
- **Database Administrator (DBA):** This position builds and maintains databases designed by the database architect and those databases that are included as a part of purchased applications. The DBA monitors databases, tunes them for performance and efficiency, and troubleshoots problems.
- **Database Analyst:** This position performs tasks that are junior to the database administrator, carrying out routine data maintenance and monitoring tasks.

(d) Network Management: Positions in network management are responsible for designing, building, monitoring, and maintaining voice and data communications networks, including connections to outside business partners and the Internet.

- **Network Architect:** This position designs data and (increasingly) voice networks and designs changes and upgrades to the network as needed to meet new organization objectives.
- **Network Engineer:** This position builds and maintains network devices such as routers, switches, firewalls, and gateways.
- **Network Administrator:** This position performs routine tasks in the network such as making minor configuration changes and monitoring event logs.
- **Telecom Engineer:** Positions in this role work with telecommunications technologies such as data circuits, phone systems, and voice email systems.

(e) Systems Management: Positions in systems management are responsible for architecture, design, building, and maintenance of servers and operating systems. This may include desktop operating systems as well.

- **Systems Architect:** This position is responsible for the overall architecture of systems (usually servers), both in terms of the internal architecture of a system, as well as the relationship between systems. This position is usually also responsible for the design of services such as authentication, e-mail, and time synchronization.
- **Systems Engineer:** This position is responsible for designing, building, and maintaining servers and server operating systems.
- **Storage Engineer:** This position is responsible for designing, building, and maintaining storage subsystems.
- **Systems Administrator:** This position is responsible for performing maintenance and configuration operations on systems.

(f) General Operations: Positions in operations are responsible for day-to-day operational tasks that may include networks, servers, databases, and applications.

- **Operations Manager:** This position is responsible for overall operations that are carried out by others. Responsibilities will include establishing operations shift schedules.
- **Operations Analyst:** This position may be responsible for the development of operational procedures; examining the health of networks, systems, and databases; setting and monitoring the operations schedule; and maintaining operations records.
- **Controls Analyst:** This position is responsible for monitoring batch jobs, data entry work, and other tasks to make sure that they are operating correctly.
- **Systems Operator:** This position is responsible for monitoring systems and networks, performing backup tasks, running batch jobs, printing reports, and other operational tasks.
- **Data Entry:** This position is responsible for keying batches of data from hard copy sources.
- **Media Librarian:** This position is responsible for maintaining and tracking the use and whereabouts of backup tapes and other media.

(g) **Security Operations:** Positions in security operations are responsible for designing, building, and monitoring security systems and security controls, to ensure the confidentiality, integrity, and availability of information systems.

- **Security Architect:** This position is responsible for the design of security controls and systems such as authentication, audit logging, intrusion detection systems, intrusion prevention systems, and firewalls.
- **Security Engineer:** This position is responsible for designing, building, and maintaining security services and systems that are designed by the security architect.
- **Security Analyst:** This position is responsible for examining logs from firewalls, intrusion detection systems, and audit logs from systems and applications. This position may also be responsible for issuing security advisories to others in IT.
- **User Account Management:** This position is responsible for accepting approved requests for user access management changes and performing the necessary changes at the network, system, database, or application level. Often this position is carried out by personnel in network and systems management functions; only in larger organizations is user account management performed in security or even in a separate user access department.
- **Security Auditor:** This position is responsible for performing internal audits of IT controls to ensure that they are being operated properly.

(h) **Service Desk:** Positions at the service desk are responsible for providing front line support services to IT and IT's customers.

- **Help desk Analyst:** This position is responsible for providing front line user support services to personnel in the organization.
- **Technical Support Analyst:** This position is responsible for providing technical support services to other IT personnel, and perhaps also to IT customers.

3.8 SEGREGATION OF DUTIES

Information systems often process large volumes of information that is sometimes highly valuable or sensitive. Measures need to be taken in IT organizations to ensure that individuals do not possess sufficient privileges to carry out potentially harmful actions on their own. Checks and balances are needed, so that high-value and high-sensitivity activities involve the coordination of two or more authorized individuals. The concept of **Segregation of Duties (SOD)**, also known as Separation of Duties, ensures that single individuals do not possess excess privileges that could result in unauthorized activities such as fraud or the manipulation or exposure of sensitive data.

The concept of segregation of duties has been long-established in organization accounting departments where, for instance, separate individuals or groups are responsible for the creation of vendors, the request for payments, and the printing of checks. Since accounting personnel frequently handle checks and currency, the principles and practices of segregation of duties controls in accounting departments are the norm.

3.8.1 Segregation of Duties Controls

Preventive and detective controls should be put into place to manage segregation of duties matters. In most organizations, both the preventive and detective controls will be manual, particularly when it comes to unwanted combinations of access between different applications. However, in some transaction-related situations, controls can be automated, although they may still require intervention by others.

3.8.2 Some Examples of Segregation of Duties Controls

♦ **Transaction Authorization:** Information systems can be programmed or configured to require two (or more) persons to approve certain transactions. Many of us see this in retail establishments where a manager is required to approve a large transaction or a refund. In IT applications, transactions meeting certain criteria (for example, exceeding normally accepted limits or conditions) may require a manager's approval to be able to proceed.

♦ **Split custody of high-value assets:** Assets of high importance or value can be protected using various means of split custody. For example, a password to an encryption key that protects a highly-valued asset can be split in two halves, one half assigned to two persons, and the other half assigned to two persons, so that no single individual knows the entire password. Banks do this for central vaults, where a vault combination is split into two or more pieces so that two or more are required to open it.

♦ **Workflow:** Applications that are workflow-enabled can use a second (or third) level of approval before certain high-value or high-sensitivity activities can take place. For example, a workflow application that is used to provision user accounts can include extra management approval steps in requests for administrative privileges.

- **Periodic reviews:** IT or internal audit personnel can periodically review user access rights to identify whether any segregation of duties issues exist. The access privileges for each worker can be compared against a segregation of duties control matrix.

When SOD issues are encountered during a segregation of duties review, management will need to decide how to mitigate the matter. The choices for mitigating a SOD issue include -

- **Reduce access privileges:** Management can reduce individual user privileges so that the conflict no longer exists.
- **Introduce a new mitigating control:** If management has determined that the person(s) need to retain privileges that are viewed as a conflict, then new preventive or detective controls need to be introduced that will prevent or detect unwanted activities. Examples of mitigating controls include increased logging to record the actions of personnel, improved exception reporting to identify possible issues, reconciliations of data sets, and external reviews of high-risk controls.

SUMMARY

In the present contemporary world, apart from change the thought-provoking terminology is business which is a driving force behind change and how to insight into trade is a dynamic called integration. Organizations of the 1990's concentrated on the re-engineering and redesign of their business processes to endorse their competitive advantage. To endure in the 21st century, organizations have started paying attention on integrating enterprise-wide technology solutions to progress their business processes called Business Information Systems (BIS). Now, every organization integrates part or all of its business functions together to accomplish higher effectiveness and yield. The thrust of the argument was that Information Technology (IT), when skillfully employed could in various ways differentiate an organization from its competition, add value to its services or products in the eyes of its customers, and secure a competitive advantage in comparison to its competition.

Although information systems have set high hopes to companies for their growth as it reduces processing speed and helps in cutting cost but most of the research studies show that there is a remarkable gap between its capabilities and the business-related demands that senior management is placing on it. We learnt how any enterprise to be effective and efficient must use Business Process Automation (BPA), which is largely aided by Computers or IT. Information systems, which forms the backbone of any enterprise comprises of various layers such as: Application software, Database Management Systems (DBMS), System Software: Operating Systems, Hardware, Network Links and People-Users.

This Chapter has provided an overview on the importance of information systems in an IT environment and how information is generated. there has been a detailed discussion on Information System Audit, its need and the method of performing the same. Chapter outlines the losses that an organization may face, incase, it does not get it audited.

TEST YOUR KNOWLEDGE

Theory Questions

1. What does an Information System Model comprise of?

   (Refer Section 3.2)

2. Discuss briefly the components of Information Systems.

   (Refer Section 3.3)

3. What do you understand by the term 'Operating System'? Discuss various operations performed by the Operating System.

   (Refer Section 3.3.2)

4. Discuss about prominent Database Models. (Refer Section 3.3.3)

5. Discuss advantages and disadvantages of Database Management Systems.

   (Refer Section 3.3.3)

6. What do you understand by Boundary Controls? Explain major Boundary Control techniques in brief.

   (Refer Section 3.4.3)

7. Briefly explain major update and report controls regarding Database Controls in brief.

   (Refer Section 3.4.3)

8. What do you mean by Corrective Controls? Explain with the help of examples. Also, discuss their broad characteristics in brief.

   (Refer Section 3.4.1)

9. What do you mean by Preventive Controls? Explain with the help of examples. Also, discuss their broad characteristics in brief.

   (Refer Section 3.4.1)

10. Write short notes on the following:

    (i) Snapshots (Refer Section 3.5.2)

    (ii) Audit Hooks (Refer Section 3.5.2)

11. What are the factors influencing an organization towards control and audit of computers?

    (Refer Section 3.5.1)

12. "Virtual Memory is in fact not a separate device but an imaginary memory area supported by some operating systems (for example, Windows) in conjunction

    with the hardware". Explain what virtual memory is and what is its importance in memory management?

    (Refer Section 3.3.2)

13. Data warehouse and Data Mining are the order of the day for better management of information and quicker and effective decision-making in organisations. Critically evaluate.

    (Refer Section 3.3)

14. Networking communication is full of some very technical concepts based on some simple principles. What are these concepts and principles behind these concepts? List ten of these and explain any five of these. (Refer to Section 3.3.4)

Multiple Choice Questions

1. Which of the following is not a component of Information Systems?

    (a) People

    (b) Data

    (c) Network

    (d) Transaction Processing System

2. Which of the following is not a functional unit of Central Processing Unit (CPU)?

    (a) Control unit

    (b) Input Devices

    (c) Registers

    (d) Arithmetic and Logic Unit

3. The full form of RAM is ___________.

   (a) Random Access Memory

   (b) Read Access Memory

   (c) Random Accessible Memory

   (d) Random Authorization Memory

4. Which of the following term is not used in Relational Database Models?

   (a) Relations

   (b) Attributes

   (c) Objects

   (d) Tables

5. Which of the following is not a Corrective Control?

   (a) Backup Procedure

   (b) Rerun Procedure

   (c) Contingency Planning

   (d) Hash Totals

6. ________ is the conversion of data into a secret code for storage in databases and transmission over networks.

   (a) Cipher Text

   (b) Encryption

   (c) Decryption

   (d) Logging

7. Under Data Coding Control, _____ occurs when a digit or character is removed from the end of a code.

   (a) Transposition Error

   (b) Substitution Error

   (c) Addition Error

   (d) Truncation Error

8. In computer networks, ________ refers to the ability of a network to recover from any kind of error like connection failure, loss of data etc.

   (a) Routing

(b) Resilience

(c) Contention

(d) Bandwidth

9. Under Application Controls, _________maintains the chronology of events that occur when a user attempts to gain access to and employ systems resources.

(a) Boundary Controls

(b) Input Controls

(c) Communication Controls

(d) Processing Controls

10. Under Application Controls, _________ maintains the chronology of events that occur either to the database definition or the database itself.

(a) Output Controls

(b) Input Controls

(c) Database Controls

(d) Processing Controls

11. Which of these is not a mobile operating system?

(a) Android

(b) iOS

(c) Tywin

(d) Windows Phone OS

12. Which of these is not an example of Relational Database?

(a) Access

(b) MySQL

(c) Java

(d) Oracle

13. Which of the following is not a step involved in the Data Mining Process?

(a) Data Integration

(b) Data Selection

(c) Data Transformation

(d) Data distribution

14. ________ technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions.

    (a) Audit hooks

    (b) SCARF

    (c) Integrated Test Facility (ITF)

    (d) Continuous and Intermittent Simulation (CIS)

15. SCARF stands for ___________.

    (a) System Control Audit Review File

    (b) System Control Audit Report File

    (c) Simulation Control Audit Review File

    (d) System Control Audit Review Format

Answers

1	(d)	**2**	(b)	**3**	(a)	**4**	(c)	**5**	(d)	**6**	(b)
7	(d)	**8**	(b)	**9**	(a)	**10**	(c)	**11**	(c)	**12**	(c)
13	(d)	**14**	(b)	**15**	(a)						

CHAPTER 4

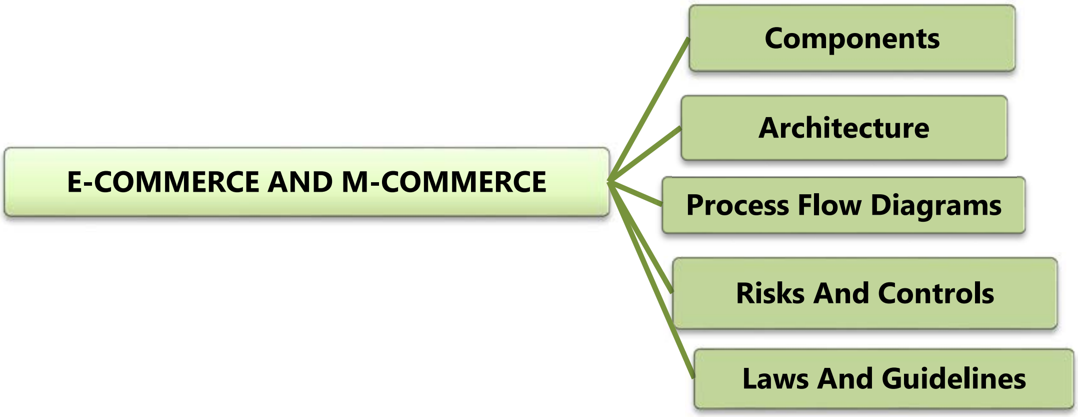
E-COMMERCE, M-COMMERCE AND EMERGING TECHNOLOGIES

LEARNING OUTCOMES

After reading this chapter, you will be able to -

- Understand the meaning, components and architecture of E-commerce.
- Grasp the knowledge about the process flows in E-commerce transactions.
- Comprehend the various aspects of risks and controls in E-commerce.
- Recognise applicable laws and guidance governing E-Commerce.
- Acknowledge a basic understanding on the paradigms of various Computing Technologies like Cloud Computing, Grid Computing, Mobile Computing, Green Computing and BYOD etc.

CHAPTER OVERVIEW



EMERGING TECHNOLOGIES

- Virtualization
- Grid Computing
- Cloud Computing
- Mobile Computing
- Green IT
- BYOD
- Web 3.0
- Artificial Intelligence
- Machine Learning

4.1 INTRODUCTION TO E-COMMERCE

E-Commerce: "Sale / Purchase of goods / services through electronic mode is e-commerce." This could include the use of technology in the form of Computers, Desktops, Mobile Applications, etc.

The greatest change due to technology innovations in last five years has been the way users perform their daily chores / activity of life. E-Commerce and its related technologies are unquestionably the current leading-edge business and finance delivery systems.

The explosion in the application of technologies and the delivery of these technologies in to the hands of consumers has made the vision, the dream, the fantasy of conducting business electronically, anywhere in the global community, a reality. E-commerce is no longer just a concept; it is a market force to be reckoned with. As more and more organizations launch Internet/ World Wide Web (WWW) home pages and intranets to disseminate company/product information, and expand their customer base, countless yet unnamed companies are just beginning to investigate this alternative. These companies are realizing that business via the Internet is inevitable that they will not be able to ignore. The lure of reaching additional customers, expanding market shares, providing value-added services, advancing technological presence, and increasing corporate profits is just too valuable to disregard, and will eventually attract companies to electronic commerce like moths to a flame.

E-Commerce is the process of doing business electronically. It refers to the use of technology to enhance the processing of commercial transactions between a company, its customers and its business partners. It involves the automation of a variety of Business-To-Business (B2B) and Business-To-Consumer (B2C) transactions through reliable and secure connections.

A recent report on India's e-Commerce growth forecasts that as a result of rising internet penetration as roughly 350 million Indian citizens are already online and that number is expected to nearly double to 600 million by 2020*. This number is more than projected users in USA by that time. Above fact is an indicator that India's e-business shall be growing very fast as internet penetration increases.

4.1.1 Traditional Commerce and E-Commerce

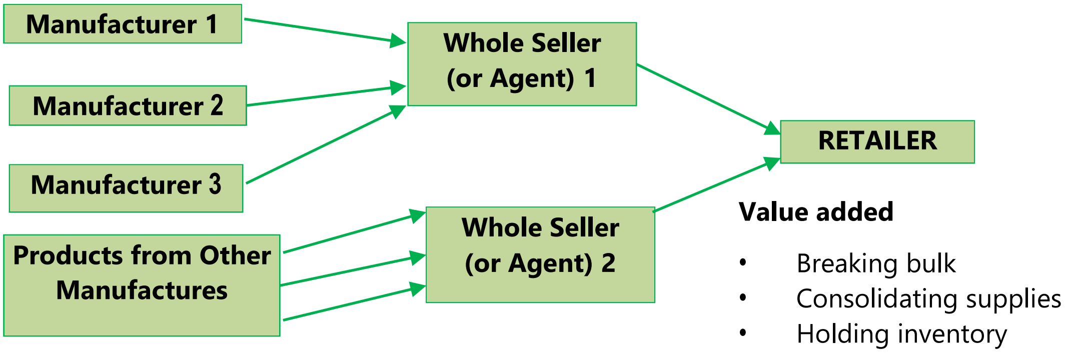
The greatest change due to technology innovations in last five years has been the way users perform their daily chores / activity of life. An illustrative Table 4.1.1 shows how technology has entered every aspect of human life.

Table 4.1.1: Example of how Technology has entered every aspect of human life

S. No.	Activity	Then	Now
1	Wake up	Alarm clocks with snooze buttons.	Mobile alarms, multiple types. Some forcing you to solve mathematical quiz before you snooze them. Ensuring you wake up.
2	Morning chores	Make / Cook Breakfast	Multiple home delivery solutions available where you can order online.

3	Going to office	In small towns in India, there was AUTO RICKSHAW	Now even in small towns you have a mobile APP through which you can call a JUGNOO auto / bike, an OLA or UBER auto / cab.
4	Office Admin	All jobs to be done by assigned service provider. For example: Courier's need to be sent to courier agency	Now you book through online APP, the courier agency picks up POST at designated time and place.
5	Procurements of all items: Items include Electronic, Furniture, Mobiles, Grocery, Cars and Bikes etc. all items covered here.	Go shop by shop to check price and quality	Now it is possible to search all products online, buyer can compare prices and order online. Few online sellers are giving facility of delivery within 12 hours of ordering.

Above is the way consumer / customers are buying products / services. This has forced organization to change their product / service delivery channels. The previous product delivery channel which was typically defined by the Fig. 4.1.1 has moved to the new product delivery model Fig. 4.1.2.


Manufacturer 1
Manufacturer 2
Manufacturer 3
Products from Other Manufactures
Whole Seller (or Agent) 1
Whole Seller (or Agent) 2
RETAILER

Value added

- Breaking bulk
- Consolidating supplies
- Holding inventory

Fig. 4.1.1: Old Model

Fig. 4.1.1 illustrates the old traditional model of doing business with multiple layers before product is finally delivered to customer. Fig. 4.1.2 illustrates the new business model enabled by technology. In this model the link to consumer and supplier is virtually direct.

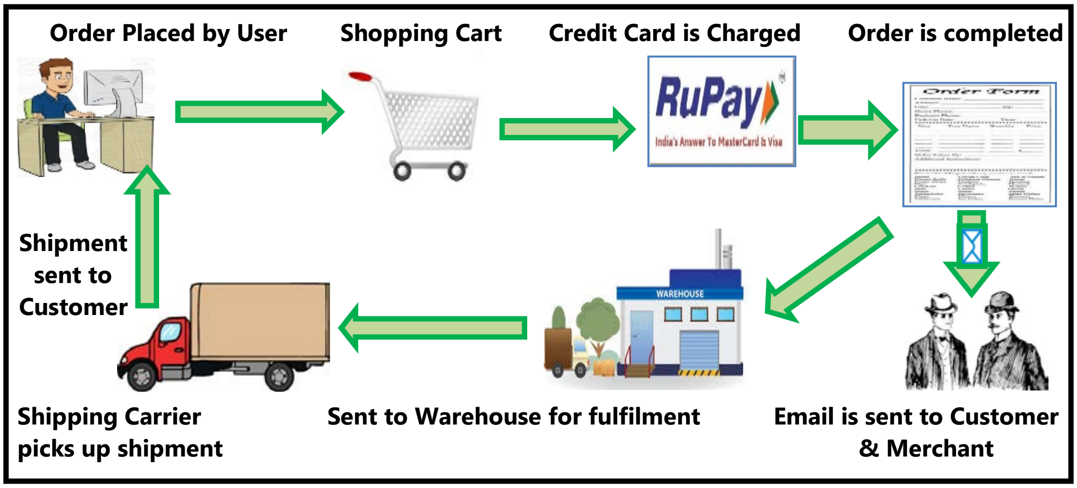

Order Placed by User
Shopping Cart
Credit Card is Charged
RuPay
India's Answer To MasterCard & Visa
Order is completed
Order Form
Shipment sent to Customer
WAREHOUSE
Shipping Carrier picks up shipment
Sent to Warehouse for fulfilment
Email is sent to Customer & Merchant

Fig. 4.1.2: New Model of E-Commerce

4.1.2 Difference between Traditional Commerce and E-Commerce

Table 4.1.2 highlights difference between Traditional Commerce and E-Commerce.

Table 4.1.2: Traditional Commerce Vs. E-Commerce

BASE FOR COMPARISON	TRADITIONAL COMMERCE	E-COMMERCE
Definition	Traditional commerce includes all those activities which encourage exchange, in some way or the other of goods / services which are manual and non-electronic.	E-Commerce means carrying out commercial transactions or exchange of information, electronically on the internet.
Transaction Processing	Manual	Electronically

Availability for commercial transactions	For limited time. This time may be defined by law. Like special stores which may run 24 hours, but in general available for limited time.	24×7×365
Nature of purchase	Goods can be inspected physically before purchase.	Goods cannot be inspected physically before purchase.
Customer interaction	Face-to-face	Screen-to-face
Business Scope	Limited to particular area.	Worldwide reach
Information exchange	No uniform platform for exchange of information.	Provides a uniform platform for information exchange.
Resource focus	Supply side	Demand side
Marketing	One way marketing	One-to-one marketing
Payment	Cash, cheque, credit card, etc.	Credit card, fund transfer, Cash in Delivery, Payment Wallets, UPCI application etc.
Delivery of goods	Instantly	Takes time, but now e-commerce websites have created options of same day delivery, or delivery within 4 hours. This option is restricted to number of cities as of now. AMAZON has already started delivery in United States of America through drones.

Fraud	Relatively lesser as there is personal interaction between the buyer and the seller.	Lack of physical presence in markets and unclear legal issues give loopholes for frauds.
Process	Because of manual processing of business transactions; chances of clerical errors are high.	Automated processing of business transactions minimizes the clerical errors. Manufacturers can have better inventory management. As they will always know what products customers are buying. They shall be able to maintain inventory on JIT (Just in Time) basis.
Profit Impact	The cost incurred on the middlemen, overhead, inventory and limited sales reduces the profit of the organization.	By increasing sales, cutting cost and streamlining operating processes - (i) The profits margin of manufacturers is increased. (ii) Above (i) allow manufacturers to give discounts to customers. (iii) Customers get better prices.

4.1.3 Illustration of E-Commerce Transaction

STEP 1: Go to website (like www.snapdeal.com, www.flipkart.com, www.amazon.in, etc) and create your user ids (identifications). Those who have social media ids, can directly link through those ids.

OR

Go to Google Play Store in your hand-held device and download the special software needed for e-commerce transaction called as APP (Application). Once downloaded, user needs to press OPEN. The APP is installed on the handheld device. For example: OYO (Hotel Booking APP), IRCTC (Train ticket booking APP), Foodpanda (Food ordering APP) and millions of APP like this.

STEP 2: Select the type of product you wish to buy. Each such e-commerce vendor has huge display of product inventory. User needs to make sure that s/he selects the right product type.

STEP 3: From the products listed, user needs to select the correct product s/he needs to buy.

STEP 4: User makes the final choice and goes for making payment online.

STEP 5: At the time of making payment, e-commerce vendor shows all details including the product being bought and the final price of the same for review of the customer and confirmation before final payment.

STEP 6: Once user goes for online payment, the e-commerce vendor displays the payment options. Payment options can be cash on delivery, Payment by Debit/Credit Cards, etc.

STEP 7: Once the user selects the payment option, he is directed to the payment gateway where he enters the OTP or the password and the payment is made vide the Credit Card. Once the payment is made, the confirmation email / SMS are received by the user.

STEP 8: Based on the delivery terms, the product is delivered to the customer in specified time.

The first e-commerce transaction vide mobile is supposed to have been done in Norway in 1997, when a Coco-Cola vending machine were configured to respond to mobile messages received from customers. The vending machine delivered products on receiving text messages.

4.1.4 Benefits of E-Business

E-business benefits individuals, businesses, government and society at large. The major benefits from e-business are as follows:

A. Benefits to Customer / Individual / User

- **Convenience:** Every product at the tip of individual's fingertips on internet.
- **Time saving:** Number of operations that can be performed both by potential buyers and sellers increase.
- **Various Options:** There are several options available for customers which are not only being easy to compare but are provided by different players in the market.

- **Easy to find reviews:** There are often reviews about a particular site or product from the previous customers which provides valuable feedback.
- **Coupon and Deals:** There are discount coupons and reward points available for customers to encourage online transaction.
- **Anytime Access:** Even midnight access to the e commerce platforms is available which brings in customer suitability.

B. Benefits to Business / Sellers

- **Increased Customer Base:** Since the number of people getting online is increasing, which are creating not only new customers but also retaining the old ones.
- **Recurring payments made easy:** Each business has number of operations being homogeneous. Brings in uniformity of scaled operations.
- **Instant Transaction:** The transactions of e commerce are based on real time processes. This has made possible to crack number of deals.
- **Provides a dynamic market:** Since there are several players, providing a dynamic market which enhances quality and business.
- **Reduction in costs:**
    - To buyers from increased competition in procurement as more suppliers are able to compete in an electronically open marketplace.
    - To suppliers by electronically accessing on-line databases of bid opportunities, on-line abilities to submit bids, and on-line review of rewards.
    - In overhead costs through uniformity, automation, and large-scale integration of management processes.
    - Advertising costs.
- **Efficiency improvement due to:**
    - Reduction in time to complete business transactions, particularly from delivery to payment.
    - Reduction in errors, time, for information processing by eliminating requirements for re-entering data.

  - ➢ Reduction in inventories and reduction of risk of obsolete inventories as the demand for goods and services is electronically linked through just-in-time inventory and integrated manufacturing techniques.

- ♦ **Creation of new markets:** This is done through the ability to easily and cheaply reach potential customers.
- ♦ **Easier entry into new markets:** This is especially into geographically remote markets, for enterprises regardless of size and location.
- ♦ **Better quality of goods:** As standardized specifications and competition have increased and improved variety of goods through expanded markets and the ability to produce customized goods.
- ♦ **Elimination of Time Delays:** Faster time to market as business processes are linked, thus enabling seamless processing and eliminating time delays.

C. Benefits to Government

- ♦ Instrument to fight corruption:-In line with Government's vision, e commerce provides a pivotal hand to fight corruption.
- ♦ Reduction in use of ecologically damaging materials through electronic coordination of activities and the movement of information rather than physical objects).

Clearly, the benefits of corporate-wide implementation of e-business are many, and this list is by no means complete. With the benefits, however, also come the risks. An organization should be cautious not to leap blindly into e-business, but rather first develop an e-business strategy, and then organize a corporate-wide team to implement that strategy.

4.1.5 E-Commerce Business Models

A Business Model can be defined as the organization of product, service and information flows, and the sources of revenues and benefits for suppliers and customers. An e-business model is the adaptation of an organization's business model to the internet economy. A Business Model is adopted by an organization as a framework to describe how it makes money on a sustainable basis and grows. A business model also enables a firm to analyze its environment more effectively and thereby exploit the potential of its markets; better understand its customers; and raise entry barriers for rivals. E-business models utilize the benefits of electronic communications to achieve the value

adding processes. Some of the e-markets are explained below in the Table 4.1.2:

Table 4.1.2: Various e-Markets

S. No.	*e-Market*	*Description*
1	*e-Shops*	*An e-shop is a virtual store front that sells products and services online. Orders are placed and payments made. They are convenient way of effecting direct sales to customers; allow manufacturers to bypass intermediate operators and thereby reduce costs and delivery times. Examples - www.sonicnet.com, www.wforwomen.com*
2	*e-Malls*	*The e-mall is defined as the retailing model of a shopping mall, a conglomeration of different shops situated in a convenient location in e-commerce.*
3	*e-auctions*	*Electronic auctions provide a channel of communication through which the bidding process for products and services can take place between competing buyers. Example – www.onsale.com*
4	*Portals*	*Portals are the channels through which websites are offered as content. The control of content can be a source of revenue for firms through charging firms for advertising or charging consumers a subscription for access.*
5	*Buyer Aggregators*	*The Buyer Aggregator brings together large numbers of individual buyers so that they can gain the types of savings that are usually the privilege of large volume buyers. In this, the firm collects the information about goods/service providers, make the providers their partners, and sell their services under its own brand. Example - www.zomato.com*
6	*Virtual Communities*	*Virtual Community is a community of customers who share a common interest and use the internet to communicate with each other. Amazon.com provides websites for the exchange of information on a wide range of subjects relating to their portfolio of products and services. Virtual communities benefit from network externalities whereby the more people who*

		join and contribute to the community, the greater the benefits that accrue, but without any additional cost to participants.
7	***e-marketing***	***e-marketing is the use of electronic communications technology such as the internet, to achieve marketing objectives. Of course, information on websites also empowers customers and helps them achieve their objectives. For example, they can compare prices of products by rival firms. The internet changes the relationship between buyers and sellers because market information is available to all parties in the transaction.***
8	***e-procurement***	***e-procurement is the management of all procurement activities via electronic means. Business models based on e-procurement seek efficiency in accessing information on suppliers, availability, price, quality and delivery times as well as cost savings by collaborating with partners to pool their buying power and secure best value deals. E-procurement infomediaries specialize in providing up-to-date and real-time information on all aspects of the supply of materials to businesses.***
9	***e-distribution***	***The e-distribution model helps distributors to achieve efficiency savings by managing large volumes of customers, automating orders, communicating with partners and facilitating value-adding services such as order tracking through each point in the supply chain. An example of a firm specializing in e-distribution is wipro.com (www.wipro.com) who use the internet to provide fully integrated e-business-enabled solutions that help to unify the information flows across all the major distribution processes including sales and marketing automation, customer service, warehouse logistics, purchasing and inventory management, and finance.***

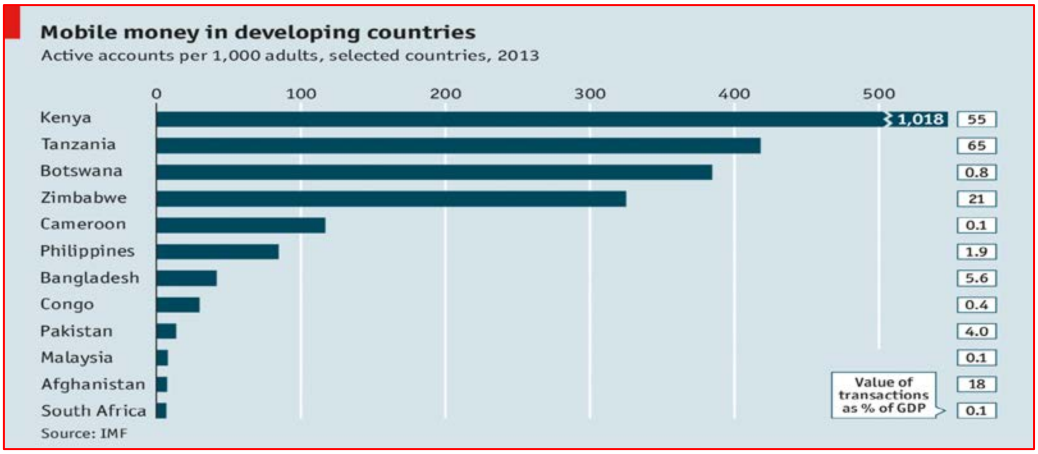
The e-business models relating to e-business markets can be summarized as given below in the Table 4.1.3.

Table 4.1.3: Some Business Models for E-Commerce

Models	***Definition***	***e-business markets***	***Examples***
Business-to-Consumer (B2C)	***Generally, this supports the activities within the customer chain in that it focuses on sell-side activities.***	***e-shops, e-malls, e-auctions, buyer aggregators, portals etc.***	***www.cisco.com www.amazon.com***
Business-to-Business (B2B)	***This supports the supply chain of organizations that involves repeat commerce between a company and its suppliers or other partners.***	***e-auctions, e-procurement, e-distribution, portals, e-marketing etc.***	***www.emall.com***
Consumer-to-Consumer (C2C)	***This supports the community plan surrounding the organization and can be seen as a commercial extension of community activities.***	***e-auctions, virtual communities etc.***	***www.eBay.com***

4.1.6 E-Commerce Future

From 1997, E-commerce has increased in leaps and bounds. Data by The Economist magazine for 2013 as shown in Fig. 4.1.3 is a pointer that E-commerce vide mobiles is not only limited to developed world. Looking to data, developing/third world countries have adopted is faster.



Source: IMF

Fig. 4.1.3: E-Commerce widespread in Developing Countries*

*Source: www.economist.com

4.2 COMPONENTS OF E-COMMERCE

Referring to the Fig, 4.2.1, E-commerce components include the following:

(i) **User:** This may be individual / organization or anybody using the e-commerce platforms. As e-commerce, has made procurement easy and simple, just on a click of button e-commerce vendors needs to ensure that their products are not delivered to wrong users. In fact, e-commerce vendors selling products like medicine / drugs need to ensure that such products are not delivered to wrong person/user.

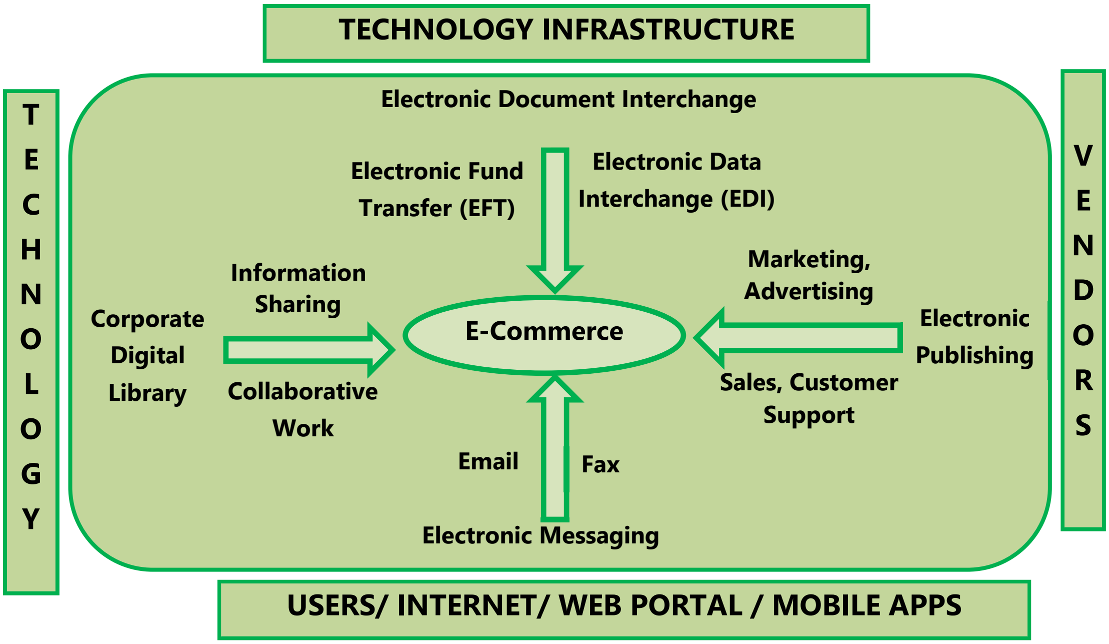

TECHNOLOGY INFRASTRUCTURE
TECHNOLOGY
Electronic Document Interchange
Electronic Fund Transfer (EFT)
Electronic Data Interchange (EDI)
Information Sharing
Corporate Digital Library
Collaborative Work
E-Commerce
Marketing, Advertising
Electronic Publishing
Sales, Customer Support
Email
Fax
Electronic Messaging
VENDORS
USERS/ INTERNET/ WEB PORTAL / MOBILE APPS

Fig. 4.2.1: Components of E - Commerce

(ii) **E-commerce Vendors:** This is the organization / entity providing the user, goods/ services asked for. For example: www.flipkart.com. E-commerce vendors further needs to ensure following for better, effective and efficient transaction.

- **Suppliers and Supply Chain Management:** These being another important component of the whole operations. For effectiveness, they need to ensure that -

  ♦ They have enough and the right goods suppliers.

  ♦ They (suppliers) are financially and operationally safe.

- ♦ Suppliers are able to provide real-time stock inventory.
- ♦ The order to deliver time is very short.

- **Warehouse operations:** When a product is bought, it is delivered from the warehouse of e-commerce vendor. This place is where online retailers pick products from the shelf, pack them as per customer's specification / pre-decided standards and prepare those products to be delivered. These operations have become very critical to the success of the whole e-commerce business. Many e-commerce companies are investing huge amounts of money in automating the whole warehouses.
- **Shipping and returns:** Shipping is supplementary and complementary to whole warehouse operations. Fast returns have become Unique Selling Preposition (USP) for many e-commerce vendors, so these vendors need very effective and efficient return processing.
- **E-Commerce catalogue and product display:** Proper display of all products being sold by vendor including product details, technical specifications, makes for a better sales conversion ratio. These help customers gauge the products/services being sold. A good catalogue makes a lot of difference to whole customer experience.
- **Marketing and loyalty programs:** Loyalty programs establish a long-term relationship with customer. The best examples can be customer loyalty programs being run by airline industry. In airline industry, customer can get good discount/ free tickets based on loyalty points accumulated. The same concept is being used by e-commerce vendors to ensure customer loyalty.
- **Showroom and offline purchase:** Few e-commerce vendors over period have realized that their products can be sold fast if customers are able to feel / touch / see those products. These vendors have opened outlets for customer experience of their products.
- **Different Ordering Methods:** These are the way customer can place his/her order, say Cash on Delivery is today most preferred method.
- **Guarantees:** The product/service guarantee associated with product/ service being sold. Money back guarantees help generate a security in customer's mind that in case of any problems, their money shall be safely returned back.
- **Privacy Policy:** Represents policy adopted by the e-commerce vendor vis-à-vis customer data/information. E-commerce website must have a privacy policy. Customers are very concerned about the information that they are

sharing. E-commerce vendors need to clearly explain them what the vendor plan to do with the various information that is collected from its customers.

- **Security:** Represents the security policy adopted by the e-commerce vendors. Vendor website needs to state that online data used to transact is safe that vendors is using appropriate security including security systems like SSL (Secure Socket Layer). This guarantees that the data provided by customer will not fall into the hand of a malicious hacker while transferring from his / her computer to the web server.

Privacy Policy and Security are also gaining importance under the Information Technology Act, 2000 (as amended 2008). The act specifically states that security of such data (the one collected by e-commerce vendor from customer) shall be responsibility of e-commerce vendor.

(iii) Technology Infrastructure: The computers, servers, database, mobile apps, digital libraries, data interchange enabling the e-commerce transactions.

(a) Computers, Servers and Database

- These are the backbone for the success of the venture. Big e-commerce organization invest huge amount of money/time in creating these systems. They store the data / program used to run the whole operation of the organization.
- As cloud computing is increasingly being used, many small / mid-sized e-commerce originations have started using shared infrastructures.

(b) Mobile Apps

Just as with the personal computer, mobile devices such as tablet computers and smart phones also have operating systems and application software. In fact, these mobile devices are in many ways just smaller versions of personal computers. A mobile app is a software application programmed to run specifically on a mobile device.

Smartphone's and tablets have become a dominant form of computing, with many more smartphones being sold than personal computers. This means that organizations will have to get smart about developing software on mobile devices in order to stay relevant. These days, most mobile devices run on one of two operating systems: Android or iOS. Android is an open-source operating system supported by Google whereas iOS is Apple's mobile operating system. There are other mobile Operating systems like BlackBerry OS, Windows Mobile, Tizen and FireFox OS.

As organizations consider making their digital presence compatible with mobile devices, they must decide whether to build a mobile app. A mobile app is an expensive proposition, and it will only run on one type of mobile device at a time. For example, if an organization creates an iPhone app, those with Android phones cannot run the application. Each app takes several thousand dollars to create, so this is not a trivial decision for many companies. One option many companies have is to create a website that is mobile-friendly. A mobile website works on all mobile devices and costs about the same as creating an app.

It includes the following:

- Mobile store front modules are an integral part of m-commerce apps, where all commodities and services are categorized and compiled in catalogs for customers to easily browse through the items on sale and get essential information about the products.
- Mobile ticketing module is an m-commerce app component that is closely linked to promotional side of commercial business and enables vendors to attract customers by distributing vouchers, coupons and tickets.
- Mobile advertising and marketing module empowers merchants to leverage m-commerce channels in order to manage its direct marketing campaigns, which are reported to be very effective especially when targeted at younger representatives of digital information consumers.
- Mobile customer support and information module is a point of reference for information about a particular retailer, its offerings and deals. The news about the company, current discounts, shop locations and other information is either pushed to users' m-commerce apps or can be found in m-commerce app itself.
- Mobile banking is inextricably linked to selling process via m-commerce apps, because no purchase can be finalized without a payment. There are various options for executing mobile payments, among which are direct mobile billing, payments via SMS, credit card payments through a familiar mobile web interface, and payments at physical POS terminals with NFC technology.

(c) **Digital Library:** A Digital Library is a special library with a focused collection of digital objects that can include text, visual material, audio material, video material, stored as electronic media formats (as opposed to print, microform, or other media), along with means for organizing, storing, and retrieving the files and media contained in the library collection. Digital libraries can vary immensely in size and scope, and can be maintained by individuals, organizations, or affiliated with established physical library buildings or institutions, or with academic institutions. The digital content may be stored locally, or accessed remotely via computer networks. An electronic library is a type of information retrieval system.

(d) **Data Interchange:** Data Interchange is an electronic communication of data. For ensuring the correctness of data interchange between multiple players in e-commerce, business specific protocols are being used. There are defined standards to ensure seamless / exact communication in e-commerce.

(iv) **Internet/Network:** This is the key to success of e-commerce transactions.

- This is the critical enabler for e-commerce. Internet connectivity is important for any e-commerce transactions to go through. Net connectivity in present days can be through traditional as well as new technology.
- The faster net connectivity leads to better e-commerce. Many mobile companies in India have launched 4G services.
- The success of e-commerce trade depends upon the internet capability of organization. At a global level, it is linked to the countries capability to create a high-speed network. The latest communication technologies like 4G, 5G have already made in-roads in India.

(v) **Web portal:** This shall provide the interface through which an individual/organization shall perform e-commerce transactions.

- Web Portal is the application through which user interacts with the e-commerce vendor. The front end through which user interacts for an e-commerce transaction. These web portals can be accessed through desktops/laptops/PDA/hand-held computing devices/mobiles and now through smart TVs also.

- The simplicity and clarity of content on web portal is directly linked to customer experience of buying a product online. E-commerce vendors put a lot of money and effort in this aspect.

(vi) **Payment Gateway:** The payment mode through which customers shall make payments. Payment gateway represents the way e-commerce / m-commerce vendors collects their payments. The payment gateway is another critical component of e-commerce set up. These are the last and most critical part of e-commerce transactions. These assures seller of receipt of payment from buyer of goods/services from e-commerce vendors. Presently numerous methods of payments by buyers to sellers are being used, including Credit / Debit Card Payments, Online bank payments, Vendors own payment wallet, Third Party Payment wallets, like SBI BUDDY or PAYTM, Cash on Delivery (COD) and Unified Payments Interface (UPI).

4.3 ARCHITECTURE OF NETWORKED SYSTEMS

Architecture is a term to define the style of design and method of construction, used generally for buildings and other physical structures. In e-commerce, it denotes the way network architectures are build.

E-commerce runs through network-connected systems. Networked systems can have two types of architecture namely;

(i) Two tier, and

(ii) Three tier.

4.3.1 Two Tier Client Server

In a **Two-tier network**, client (user) sends request to Server and the Server responds to the request by fetching the data from it. The Two-tier architecture is divided into two tiers- **Presentation Tier** and **Database Tier** as shown in the Fig. 4.3.1.

(i) **Presentation Tier (Client Application/Client Tier):** This is the interface that allows user to interact with the e-commerce / m-commerce vendor. User can login to an e-commerce vendor through this tier. This application also connects to database tier and displays the various products / prices to customers.

(ii) **Database Tier (Data Tier):** The product data / price data / customer data and other related data are kept here. User has not access to data / information at this level but he/she can display all data / information stored here through application tier.

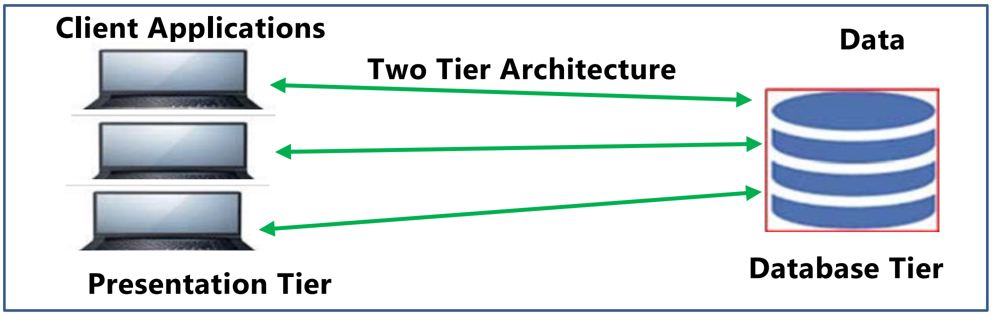


Fig. 4.3.1: Two Tier Client Server Architecture

The **Advantages of Two-Tier Systems** are as follows:

- The system performance is higher because business logic and database are physically close.
- Since processing is shared between the client and server, more users could interact with system.
- By having simple structure, it is easy to setup and maintain entire system smoothly.

The **Disadvantages of Two-Tier Systems** are as follows:

- Performance deteriorates if number of users' increases.
- There is restricted flexibility and choice of DBMS, since data language used in server is proprietary to each vendor.

4.3.2 Three Tier Client Server

Three - Tier architecture is a software design pattern and well-established software architecture. Its three tiers are the **Presentation Tier**, **Application Tier** and **Data Tier**. Three-tier architecture is a client-server architecture in which the functional process logic, data access, computer data storage and user interface are developed and maintained as independent modules on separate platforms. The three-tier architecture is shown in Fig. 4.3.2 and explained below:

(i) **Presentation Tier:** Occupies the top level and displays information related to services available on a website. This tier communicates with other tiers by sending results to the browser and other tiers in the network.

(ii) **Application Tier:** Also, called the **Middle Tier**, **Logic Tier**, **Business Logic** or **Logic Tier**; this tier is pulled from the Presentation tier. It controls application functionality by performing detailed processing. In computer software, business logic or domain logic is the part of the program that encodes the real-world business rules that determine how data can be created, displayed, stored and changed.

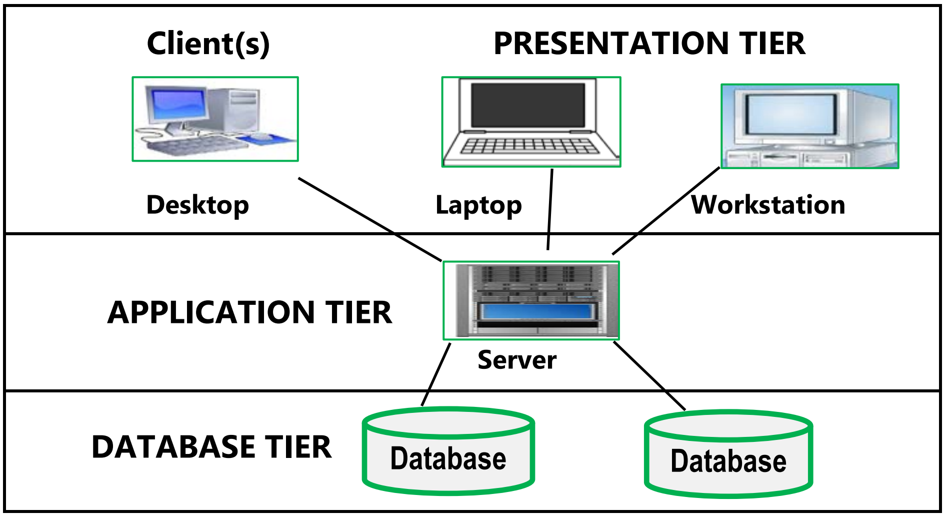


Fig. 4.3.2: Three-Tier Client Server Architecture

(iii) Database Tier: This tier houses the database servers where information is stored and retrieved. Data in this tier is kept independent of application servers or business logic. The Data Tier includes the data persistence mechanisms (database servers, file shares, etc.) and the data access layer that encapsulates the persistence mechanisms and exposes the data. The data access layer should provide an Application Programming Interface (API) to the application tier that exposes methods of managing the stored data without exposing or creating dependencies on the data storage mechanisms. Avoiding dependencies on the storage mechanisms allows for updates or changes without the application tier clients being affected by or even aware of the change. To conclude, in Three Tier Architecture three layers like Client, Server and Database are involved. In this, the Client sends a request to Server, where the Server sends the request to Database for data, based on that request the Database sends back the data to Server and from Server the data is forwarded to Client.

The following are the **Advantages of Three-Tier Systems**:

- **Clear separation of user-interface-control and data presentation from application-logic:** Through this separation more clients can have access to a wide variety of server applications. The two main advantages for client-applications are quicker development through the reuse of pre-built business-logic components and a shorter test phase.

- **Dynamic load balancing:** If bottlenecks in terms of performance occur, the server process can be moved to other servers at runtime.
- **Change management:** It is easy and faster to exchange a component on the server than to furnish numerous PCs with new program versions.

The **Disadvantages of Three-Tier Systems** are as follows:

- It creates an increased need for network traffic management, server load balancing, and fault tolerance.
- Current tools are relatively immature and are more complex.
- Maintenance tools are currently inadequate for maintaining server libraries. This is a potential obstacle for simplifying maintenance and promoting code reuse throughout the organization.

4.3.3 Which Architecture is used?

In two tier architectures, application performance will be degraded upon increasing the users and it is cost in-effective whereas a three-tier architecture provides High performance, lightweight persistent objects, flexibility, maintainability, reusability and scalability, performance, high degree of flexibility in deployment, better Re-use, improved data integrity, improved security wherein client does not have direct access to database, easy to maintain and application performance is good. Apart from the usual advantages of modular software with well-defined interfaces, the three-tier architecture is intended to allow any of the three tiers to be upgraded or replaced independently in response to changes in requirements or technology.

All e-commerce applications follow the three-tier network architecture.

4.3.4 E-Commerce Architecture Vide Internet

Fig. 4.3.3 depicts the E-commerce architecture vide Internet and Table 4.3.1 elaborates the functioning of each layer.

Table 4.3.1: Description of each Layer as per Fig. 4.3.3

S. No.	Layer	Includes	Purpose
1	Client/ User Interface	Web Server, Web Browser and Internet. For example: In example (Fig. 4.3.3) where user buys a mobile phone	This layer helps the e-commerce customer connect to e-commerce merchant.

		from an e-commerce merchant it includes - User, Web Browser (Internet Explorer/Chrome) & Web Server	
2	Application Layer	Application Server and Back End Server. For example - In the same example, it includes: - E-merchant - Reseller - Logistics partner	Through these application's customer logs to merchant systems. This layer allows customer to check the products available on merchant's website.
3	Database Layer	The information store house, where all data relating to products and price is kept.	This layer is accessible to user through application layer.

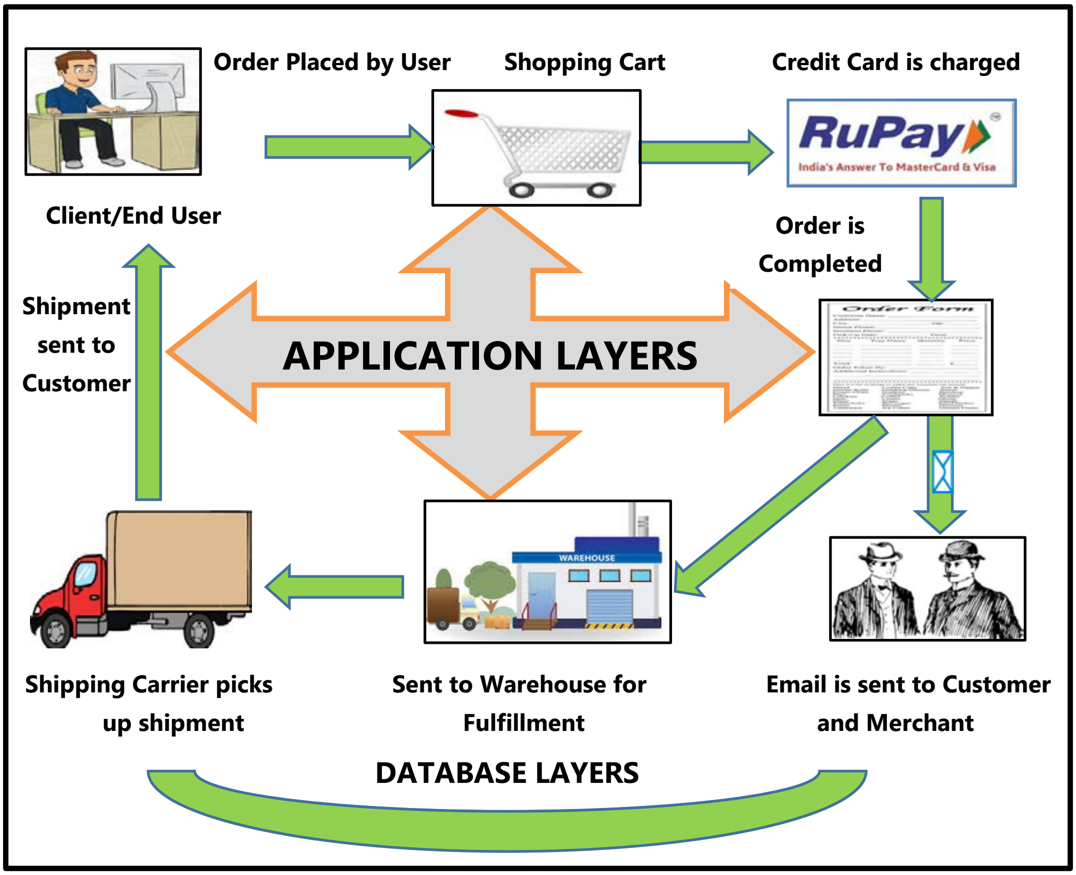

Order Placed by User
Shopping Cart
Credit Card is charged
RuPay
India's Answer To MasterCard & Visa
Client/End User
Order is Completed
Shipment sent to Customer
APPLICATION LAYERS
Order Form
WAREHOUSE
Shipping Carrier picks up shipment
Sent to Warehouse for Fulfillment
Email is sent to Customer and Merchant
DATABASE LAYERS

Fig. 4.3.3: E-commerce Vide Internet

4.3.5 E-Commerce Architecture Vide Mobile Apps

M-Commerce (Mobile Commerce): M-commerce (mobile commerce) is the buying and selling of goods and services through wireless handheld devices such as cellular telephone and Personal Digital Assistants (PDAs). M-commerce enables users to access the Internet without needing to find a place to plug in. Refer Fig. 4.3.4 for E-Commerce vide Mobile Apps.

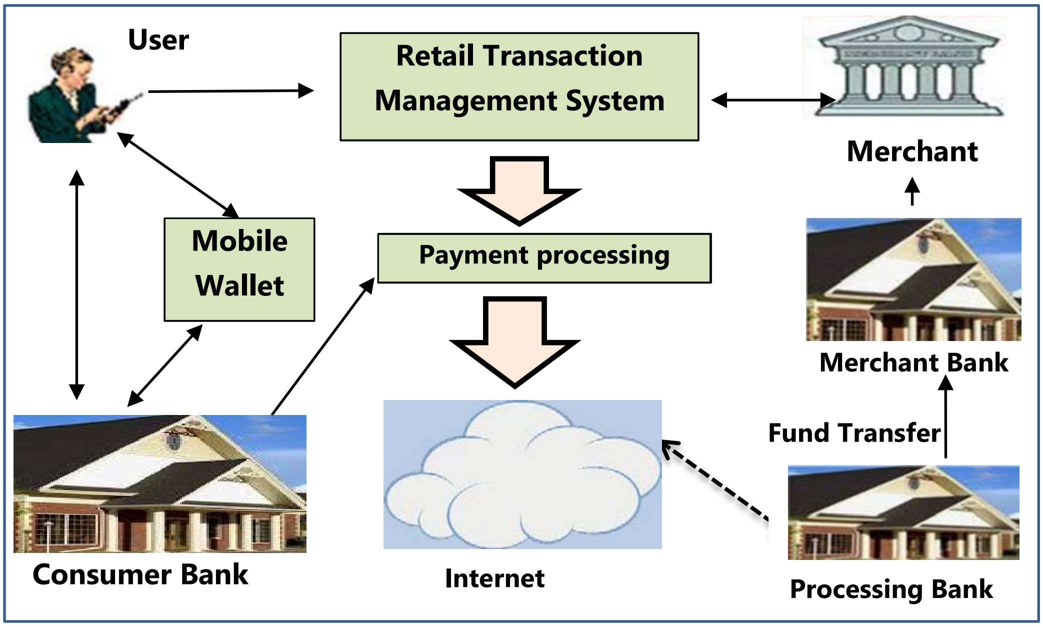


Fig. 4.3.4: E- commerce Vide Mobile Apps

The key growth in the mobile e-Commerce sector in recent years has been in through so-called <u>Apps</u>. Apps, short for Mobile Applications, are small piece of software developed specifically for the operating systems of handheld devices such as mobile phones, PDAs and Tablet computers. Mobile Apps can come preloaded on handheld devices or can be downloaded by users from the app stores over the Internet.

Table 4.3.2: Description of Fig. 4.3.4

S. No.	Layer	Includes	Purpose
1	Client / User Interface	Mobile Web Browser and Internet. For example: In example discussed above where user	This layer helps the e-commerce customer connect to e-commerce merchant.

		buys a mobile phone from e-commerce merchant; it includes: - Mobile App (Application) - User	
2	Application Layer	Application Server and back end server. For example: In the same example, it includes - E-merchant - Reseller - Logistics partner - Payment Gateway	Through these application's customer logs to merchant systems. This layer allows customer to check the products available on merchant's website.
3	Database Layer	The information store house, where all data relating to products, price it kept.	This layer is accessible to user through application layer.

4.4 WORK FLOW DIAGRAM FOR E-COMMERCE

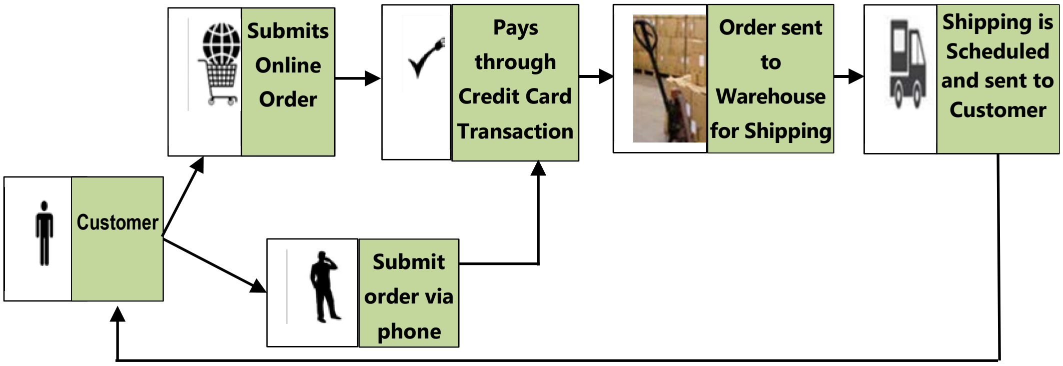

Submits Online Order
Pays through Credit Card Transaction
Order sent to Warehouse for Shipping
Shipping is Scheduled and sent to Customer
Customer
Submit order via phone

Fig. 4.4.1: E-Commerce Workflow Diagram*

Refer Fig. 4.4.1 for E-Commerce Work Flow and Table 4.4.1 for its description.

* source: www.juanribon.com

Table 4.4.1: Description of E-Commerce Work Flow Diagram

S. No.	Step	Activities
1	Customers login	Few e-commerce merchants may allow same transactions to be done through phone, but the basic information flow is e-mode.
2	Product / Service Selection	Customer selects products / services from available options.
3	Customer Places Order	Order is placed for selected product / service by customer. This step leads to next important activity PAYMENT GATEWAY.
4	Payment Gateway	Here customer makes a selection of the payment method. In case payment methods is other than cash on delivery(COD), the merchant gets the update from payment gateway about payment realisation from customer. In case of COD, e-commerce vendor may do an additional check to validate customer.
5	Dispatch and Shipping Process	This process may be executed at two different ends. First if product / service inventory is managed by e-commerce vendor, then dispatch shall be initiated at merchant warehouse. Second, many e-commerce merchants allow third party vendors to sale through merchant websites. For example: FLIPKART states that it has more than 1 lac registered third party vendors on its website.
6	Delivery Tracking	Another key element denoting success of e-commerce business is timely delivery. Merchants keep a track of this. All merchants have provided their delivery staff with hand held devices, where the product / service delivery to customers are immediately updated.
7	COD tracking	In case products are sold on COD payment mode, merchants need to have additional check on matching delivery with payments.
Numerous services are of the nature which does not have a separate delivery need, for example booking a train ticket through irctc.co.in. In this case, there is no separate delivery of service, tickets booking updates are generated as soon as payments are received by irctc.co.in payment gateways.		

4.5 RISKS AND CONTROLS RELATED TO E-COMMERCE

4.5.1 Risks in an e-Business Environment

Risk is possibility of loss. The same may be result of intentional or un-intentional action by individuals. Risks associated with e-commerce transactions are high compared to general internet activities. These include the following:

(i) **Privacy and Security:** There are often issues of security and privacy due to lack of personalized digital access and knowledge.

(ii) **Quality issues:** There are quality issues raised by customers as the original product differs from the one that was ordered.

(iii) **Delay in goods and Hidden Costs:** When goods are ordered from another country, there are hidden costs enforced by Companies.

(iv) **Needs Access to internet and lack of personal touch:** The e-commerce requires an internet connection which is extra expensive and lacks personal touch.

(v) **Security and credit card issues:** There is cloning possible of credit cards and debit cards which poses a security threat.

(vi) **Infrastructure:** There is a greater need of not only digital infrastructure but also network expansion of roads and railways which remains a substantial challenge in developing countries.

(vii) **Problem of anonymity:** There is need to identify and authenticate users in the virtual global market where anyone can sell to or buy from anyone, anything from anywhere.

(viii) **Repudiation of contract:** There is possibility that the electronic transaction in the form of contract, sale order or purchase by the trading partner or customer maybe denied.

(ix) **Lack of authenticity of transactions:** The electronic documents that are produced during an e-Commerce transaction may not be authentic and reliable.

(x) **Data Loss or theft or duplication:** The data transmitted over the Internet may be lost, duplicated, tampered with or replayed.

(xi) **Attack from hackers:** Web servers used for e-Commerce maybe vulnerable to hackers.

(xii) **Denial of Service:** Service to customers may be denied due to non-availability of system as it may be affected by viruses, e-mail bombs and floods.

(xiii) **Non-recognition of electronic transactions:** e-Commerce transactions, as electronic records and digital signatures may not be recognized as evidence in courts of law.

(xiv) **Lack of audit trails:** Audit trails in e-Commerce system may be lacking and the logs may be incomplete, too voluminous or easily tampered with.

(xv) **Problem of piracy:** Intellectual property may not be adequately protected when such property is transacted through e-Commerce.

4.5.2 Control in an e-Business Environment

Internal Control, as defined in accounting and auditing, is a process for assuring achievement of an organization's objectives in operational effectiveness and efficiency, reliable financial reporting, and compliance with laws, regulations and policies. For example:

- Company may have a policy to force employees to change their passwords every 30 days.
- A CA firm may not allow office staff access to social sites during office hours.

In an e-business environment, controls are necessary for all persons in the chain, including-

A. **Users:** This is important to ensure that the genuine user is using the e-commerce/ m-commerce platform. There is risk if user accounts are hacked and hackers buy products / services.

B. **Sellers / Buyers / Merchants:** These people need to proper framework in place to ensure success of business. Many e-commerce businesses have lost huge amount of money as they did not have proper controls put in place. These include controls on:

a. Product catalogues

b. Price catalogues

c. Discounts and promotional schemes

d. Product returns

e. Accounting for cash received through Cash on Delivery mode of sales.

C. **Government:** Governments across the world and in India have few critical concerns vis-à-vis electronic transactions, namely:

a. Tax accounting of all products / services sold.

b. All products / services sold are legal. There have been instances where narcotics drugs have found to be sold and bought through electronic means.

D. **Network Service Providers:** They need to ensure availability and security of network. Any downtime of network can be disastrous for business.

E. **Technology Service Providers:** These include all other service provider other than network service provider, for example, cloud computing back-ends, applications back-ends and like. They are also prone to risk of availability and security.

F. **Logistics Service Providers:** Success or failure of any e-commerce / m-commerce venture finally lies here. Logistics service providers are the ones who are finally responsible for timely product deliveries.

G. **Payment Gateways:** E-commerce vendors' business shall run only when their payment gateways are efficient, effective and foolproof.

Each participant needs to put in place controls in an e-commerce environment. Any lack of exercising controls by anyone can bring the risk to whole chain. All participants as discussed above need to trained and educated for proper controls. Each participant needs to put in place policies, practices and procedures in place to protect from e-commerce / m-commerce related risks. These will include the following:

1. **Educating the participant about the nature of risks.**

Every participant needs to be educated / sensitized towards risk associated with such transactions. Organizations need to put in place infrastructure / policy guidelines for the same. These policies may include the following:

- Frequency and nature of education programs.
- The participants for such program.

For example: All bank in India, allowing on line payments put ads on their websites "Dos and Don'ts for online payments." The more informed your organization is, the easier it will be to combat online threats and to carry out risk mitigating measures.

2. **Communication of organizational policies to its customers.**

   To avoid customer dissatisfaction and disputes, it is necessary to make the following information clear throughout your website:

   - **Privacy Policies:** These should be available through links on any website.
   - **Information security:** Create a page that educates customers about any security practices and controls.
   - **Shipping and billing policies:** These should be clear, comprehensive and available through a link on the home page during online purchase.
   - **Refund policies:** Establish and display a clear, concise statement of a customer's refund and credit policy.

3. **Ensure Compliance with Industry Body Standards.**

   All e-Commerce organizations are required to be complying with and adhere to the rules outlined by the law of land. In India Reserve Bank of India, has been releasing these standards from time to time.

4. **Protect your e-Commerce business from intrusion.**

   a. **Viruses:** Check your website daily for viruses, the presence of which can result in the loss of valuable data.

   b. **Hackers:** Use software packages to carry out regular assessments of how vulnerable your website is to hackers.

   c. **Passwords:** Ensure employees change these regularly and that passwords set by former employees of your organization are defunct.

   d. **Regular software updates:** Your site should always be up to date with the newest versions of security software. If you fail to do this, you leave your website vulnerable to attack.

   e. **Sensitive data:** Consider encrypting financial information and other confidential data (using encryption software). Hackers or third parties will not be able to access encrypted data without a key. This is particularly relevant for any e-Commerce sites that use a shopping cart system.

   f. Know the details of your payment service provider contract.

4.5.3 Case Studies

Case 1: Return of Mobile

A person in Hyderabad was caught for returning mobiles with defective parts.

Modus operandi:

- He used to buy new mobile online from India's largest m-commerce vendor.
- Return them with complaint that mobile purchased is defective.
- He used to replace the new mobiles internal components with defective components.
- He kept on doing this for two years before being caught.

What control lapse lead to above fraud?

- Entities poor policy documentation regarding accepting mobile returns as defective.
- Within the organization there must have been a person putting a red mark when the same person was returning mobiles as defective. This reflects poor audit mechanism.

Case 2: Purchase fake/inferior products online.

Certain websites allow anybody to sell products on, which creates a market for fake and bootleg products. It is important to check the history of the seller and read all the details to ensure the product is the brand name product you originally intended to buy. A good rule of thumb is that if it's too good to be true, it usually is. Designer headphones, purses and watches will always cost around retail price online.

4.5.4 Cyber Security Risk Considerations

The business and technological environment in which the entities operate are rapidly changing on account of the E-Commerce platforms on which most of them now operate. Therefore, it is imperative for the consideration of Cyber Security Risks in the audit procedures.

Risk Assessment is always a very important part and parcel of the audit procedures. One of the most important aspects to be kept in mind during the risk assessment process is giving due consideration to the changing risks in the entity and its environment due to the ever-evolving technology landscape which can have a potential impact on the financial statements. There could be cyber security risks with **Direct** as well as **Indirect** impact.

- A **Direct Financial Impact** could be if the Application at the Company's Retailers which contains financial information has weak passwords at all Open Systems Interconnection (OSI) layers resulting in harming the integrity of data.
- An **Indirect Operational Impact** could be if the sensitive customer information in the form of Bank Account Numbers Recipes of Patented products, etc. could be breached which would result in legal and regulatory actions on the Company on account of breach of confidential information.

(Standard on Auditing) SA 315 recognizes that IT poses specific risks to an entity's Internal Control in the form of the following:

- Reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both.
- Unauthorized access to data that may result in destruction of data or improper changes to data, including the recording of unauthorized or non-existent transactions, or inaccurate recording of transactions. Particular risks may arise where multiple users access a common database.
- The possibility of IT personnel gaining access privileges beyond those necessary to perform their assigned duties thereby breaking down segregation of duties.
- Unauthorized changes to data in master files.
- Unauthorized changes to systems or programs.
- Failure to make necessary changes to systems or programs.
- Inappropriate manual intervention.
- Potential loss of data or inability to access data as required.

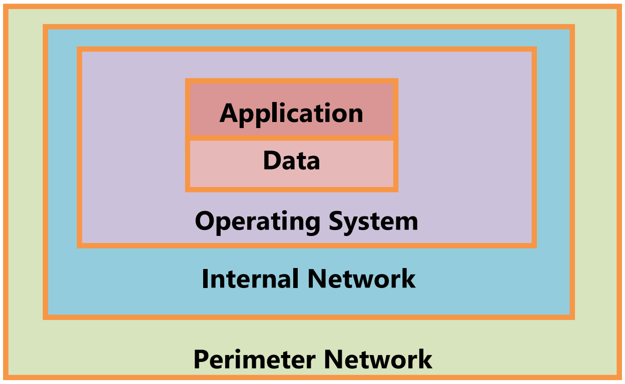


Fig. 4.5.1: Levels through which Cyber breach can occur

Referring to the Fig. 4.5.1, it is interesting to note that cyber breach incidents usually occur through the Perimeter and Internal Network and then go on to the Application and Database which store the financial information. Illustrations of the considerations as controls addressing key cyber security risks are as under:

(i) A Network Diagram detailing server, databases, hubs, routers, internal and external network, etc.

(ii) List of the Digital Assets used by the Company and the IT Managers responsible for the protection for those digital assets along with the physical location of those assets.

(iii) Policy and Procedure document of the criticality of the Digital Assets, the use of those digital assets, any direct impact on the financial statements of the company, access restrictions to those assets.

(iv) Any incidents of cyber security breach which occurred and the actions taken and controls built in to avoid them from occurring again.

(v) Annual review by the CIO, based on the Company's digital assets and the IT Environment in which it operates assessing which are the most critical cyber security risks and designing controls to address the same.

(vi) Are the IT managers responsible for the safeguarding of the assets from cyber-attacks, adequately skilled and trained to perform the functions.

(vii) The Entity should have a IT Security Policy circulated to all Employees detailing the procedures to be adhered to when accessing IT systems/ resources like password security, restricted use of internet, etc.

(viii) Periodical review of access rights to all IT resources to ensure that the access to the users is commensurate with their functional roles and responsibilities.

(ix) Adequate approvals exist before the access is granted to any IT resources.

(x) Timely employee awareness campaigns focusing on methods of intrusion which can be stopped based on individual actions.

(xi) Use of firewalls by the Company to allow internet activity in accordance with the rules defined.

(xii) Any baseline security configurations established by the Company under any security standards which are periodically reviewed.

(xiii) All remote access logins are configured for two factor' authentications like - using of username, password, pin, token, etc.

(xiv) Any vulnerability scans or penetration testing performed by the Company and any findings noted.

(xv) Are the backups scheduled properly and timely checked by restoration of data?

The above procedures are even to be considered for the assets not owned by the Company but where the Company is utilizing services from another service provider like the Server maintenance and security is outsourced to an outsourced service provider.

4.6 GUIDELINES AND LAWS GOVERNING E-COMMERCE

4.6.1 Guidelines for E-Commerce

All entity going for e-commerce / m-commerce business needs to create clear policy guidelines for the following:

1. **Billing:** The issues are -
    a. Format of bill
    b. The details to be shared in bills.
    c. Applicable GST.
2. **Product guarantee / warranty:** Proper display of product guarantee / warranty online as well as documents sent along with the products.
3. **Shipping:** The shipping time, frequency of shipping, the packing at time of shipping, all these needs to be put in policy documents. This will ensure products are properly packed and timely shipped.
4. **Delivery:** Policy needs to be defined for:
    a. Which mode of delivery to be chosen? Say through courier / third party had delivery / own staff hand delivery
    b. When deliveries to be made? Say time of day.
    c. Where deliveries to be made? Say buyer's office / home or through dedicated delivery shops. Many e-commerce companies in India have started creating delivery shops in metro cities. These delivery centers are in big residential townships. The buyer shall take delivery of products from these centers.

5. **Return:** Policy for return of goods need to be put in place defining:

   a. Which goods to be accepted in return? Food products would generally not be accepted.

   b. The number of days within which returns can be accepted.

   c. The process of verifying the authenticity of products received back.

   d. The time within which buyer shall be paid his/her amount back for goods returned.

6. **Payment:** Policy guidelines need to be created for the following payment related issues:

   a. Mode of payment.

   b. For which products, specific payment mode shall be there. Organization restricts cash on delivery for few consumable products.

4.6.2 Commercial Laws Governing E-Commerce

All e-commerce transactions are commercial business transactions. All these transactions are covered under multiple laws, including commercial laws. Following commercial laws are applicable to e-commerce and m-commerce transactions.

♦ **Income Tax Act, 1961:** Income Tax Act, has detailed provisions regarding taxation of income in India. In respect of e-commerce / m-commerce transactions, the issue of deciding place of origin transaction for tax purpose is critical.

♦ **Companies Act, 2013:** Companies Act, 2013, regulates the corporate sector. The law defines all regulatory aspects for companies in India. Most of the merchants in e-commerce / m-commerce business are companies, both private and public.

♦ **Foreign Trade (Development and Regulation) Act, 1992:** An Act to provide for the development and regulation of foreign trade by facilitating imports into, augmenting exports from, India and for matters connected therewith or incidental thereto. Amazon has recently allowed Indian citizens to purchase from its global stores. All these shall be regulated through above law.

♦ **The Factories Act, 1948:** Act to regulate working conditions of workers. The act extends to place of storage as well as transportation. Most of the merchants in e-commerce / m-commerce business need to comply with provisions of the act.

- **The Custom Act, 1962:** The act that defines import / export of goods / services from India and provides for levy of appropriate customs duty. India being a signatory to General Agreement on Trade and Tariff (GATT) under World Trade Organization, cannot levy any custom duty that GATT non-compliant. This one law is subject to debate across the world. For example: An Indian company downloads software being sold by a foreign company whether the same shall be chargeable to duty of import.
- **The Goods and Services Tax (GST) Law:** This Law requires each applicable business, including e-commerce/ m-commerce, to upload each sales and purchase invoice on one central IT infrastructure, mandating reconciliations of transactions between business, triggering of tax credits on payments of GST, facilitating filling of e-returns, etc.
- **Indian Contract Act,1872:** The Act defines constituents of a valid contract. In case of e-commerce / m-commerce business, it becomes important to define these constituents.
- **The Competition Act, 2002:** Law to regulate practices that may have adverse effect on competition in India. Competition Commission have been vigilant to ensure that e-commerce / m-commerce merchants do not engage in predatory practices.
- **Foreign Exchange Management Act (FEMA 1999):** The law to regulate foreign direct investments, flow of foreign exchange in India. The law has important implications for e-commerce / m-commerce business. With a view to promote foreign investment, as per regulations framed under Foreign Exchange Management Act, (FEMA) 1999, FDI up to 100% under the automatic route is permitted in companies engaged in e-commerce provided that such companies would engage in Business to Business (B2B) e-commerce. Foreign investment in Business to Customer (B2C) e-commerce activities has been opened in a calibrated manner and an entity is permitted to undertake retail trading through e-commerce under the following circumstances:

  (i) A manufacturer is permitted to sell its products manufactured in India through e-commerce retail.

  (ii) A single brand retail trading entity operating through brick and mortar stores, is permitted to undertake retail trading through e-commerce.

  (iii) An Indian manufacturer is permitted to sell its own single brand products through e-commerce retail. Indian manufacturer would be the investee company, which is the owner of the Indian brand and which manufactures in India, in terms of value, at least 70% of its products in house, and sources, at most 30% from Indian manufacturers.

- **Consumer Protection Act, 1986:** The law to protect consumer rights has been source of most of litigations for transaction done through e-commerce and m-commerce.

All laws above have same nature of applicability as in a normal commercial transaction. The fact that transactions are done electronically gives rise to issues which are unique in nature. Few of issues have been put to rest by court decisions but new issues crop up every day. An illustrative list of such issues is discussed in the Table 4.6.1.

Table 4.6.1: Illustrative List of Issues during an Online Transaction

S. No.	**Event**	**Legal questions out of event**
1	Product ordered by **'A'** delivered to **'B'**. (For example: a DEO). **'A'** had made payment online.	1. What if **'B'** accepts the products and starts using? 2. **'A'** had ordered the product to gift to spouse on his/her birthday. What of the mental agony caused? 3. The product is a medicine necessary of treatment of **'A's** dependent parents. In case of any complication to **'A's** parent due to delayed delivery who bears the additional medical costs? Above is only an illustrative list. Imagine numerous possible combinations based on fact of in-correct delivery.
2	Service ordered by **'A'** not provided by online vendor. For example: **'A'** courier company does not collect an important document.	1. Who bears the loss that may be incurred by **'A'**?
3	**'A'** auction website sales in-advertently sales products which cannot be sold at all, or sale of those	1. What is the legal liability if seller of products? 2. What is legal liability of buyers of such products?

	products is illegal. For example: Guns/ Narcotics Drugs.	3. What is the legal liability of auction website?
4	**‘A’** downloads a software from a server in USA. **‘A’** is in state of MP and then he sells the software to a person in Mumbai or Sells the same to another person in Singapore.	1. Whether such a download is import? 2. If **‘A’** re-exports can s/he claim benefits under customs?

4.6.3 Special Laws governing E-Commerce

E-commerce are covered under few other laws as these transactions are done electronically.

- Information Technology Act, 2000 (As amended 2008)
- Reserve Bank of India, 1934.

I. Information Technology Act, 2000

This law governs all internet activities in India. The law is applicable to all online transactions in India, and provides for penalties, prosecution for non-compliances. The important issues dealt in by the law includes:

- Legality of products / services being offered online.
- Data Protection
- Protecting Your Customer’s Privacy Online
- Online Advertising Compliance
- Compliance with Information Technology Act, provisions.

II. Reserve Bank of India, 1934

Reserve Bank of India (RBI), from time to time frames guidelines to be followed by e-commerce / m-commerce merchants allowing online payments through various modes. The merchant needs to comply with these guidelines. For example:

- The conversion of all Credit / Debit cards to be made CHIP based.
- An OTP / PIN for all transactions done on point of sale machines through debit / credit cards.

- The compliance with capital adequacy norms for payments wallet like SBI BUDDY/ PAYTM etc.

Case 1: Delivering soap instead of mobile phone.

The police in Mumbai have registered a case of cheating against online shopping portal for delivering a bar of soap to a customer who had ordered a Samsung Galaxy Note 4. Mr. A, a resident of Walkeshwar, was excited to receive the parcel, but was shocked to find a bar of Nirma soap instead. Mr. A, who works at a leading global IT firm, decided to register the complaint after the company initially said his complaint was not genuine.

"I had ordered a Samsung Galaxy Note 4 on May 25 and the product was delivered on May 30. I had opted for cash-on-delivery and paid ₹ 29,900 to the delivery boy," Mr. A informed.

Minutes later, he opened the box and saw it contained a bar of soap in place of the smartphone. "The box contained a soap bar and an Android phone charger. I telephoned the deliveryman immediately. He was 10 minutes away from my home but said I would have to call Flipkart's customer care number to lodge a complaint".

He called the customer care but was shocked when he was told his complaint was not genuine. He reported the matter to the Malabar Hill police and lodged a complaint, after which a first-information report under Section 420 (cheating and dishonestly inducing delivery of property) of the Indian Penal Code was registered.

"My experience with online retailer has been disgusting. I received Nirma soap instead of a smartphone. Over the next few days I called them several times to inquire about the issue but received neither the cell phone nor my money. They initially denied me a refund or replacement, claiming that my complaint was not genuine. This was very annoying, so I filed a complaint with the police and on various customer complaint websites, after which they refunded my money on Tuesday," Mr. A said.

"We will begin our investigation by taking the statement of the delivery boy, after which we will look into other aspects of the case," police sub-inspector said.

For its part, online retailer said in written statement: "The company observes a zero-tolerance policy on incidents that impact customer trust. We are conducting an internal investigation into this case and are putting all efforts to find out the real facts of this incident. Meanwhile, as a responsible marketplace, the money has been refunded to the customer in good faith."

Case 2: Online Retailer not being paid by companies putting ads on online retailer's portal.

India's top online retailer filed first such case in the Delhi High Court against a US-based computer data storage company WD for allegedly not paying more than ₹ 1 crore for placing advertisements on the retailer's website.

4.7 DIGITAL PAYMENTS

Digital Payment is a way of payment which is made through digital modes. In digital payments, payer and payee both use digital modes to send and receive money. It is also called electronic payment. No hard cash is involved in the digital payments. All the transactions in digital payments are completed online. It is an instant and convenient way to make payments.

New digital payment platforms such as UPI and IMPS are becoming increasingly popular. Using these new platforms, banks have been scaling rapidly. Every Bank is impacted by new digital disruptions, so new banking services and ways should be adapted to use various digital channels to interact and provide services to customers. To reach out to customers at their convenience, banks are aggressively going digital. For millennials, banking is all about convenience – a seamless user interface akin to that of games or app. They value transparency and minimal processes. Convenience can be delivered through mobile apps and digital banking, the latter is provided by relationship managers, who need to be proficient in products and process knowledge. A high level of adaptability is a must for banking sector in this highly digital and tech-savvy age, where banking transactions can happen even on a mobile or tablet with a few clicks.

4.7.1 Different Types of Digital Payments

From traditional digital payment methods, India is moving towards newer methods of digital payments.

I. New Methods of Digital Payment

(i) UPI Apps: Unified Payment Interface (UPI) and retail payment banks are changing the very face of banking in terms of moving most of banking to digital platforms using mobiles and apps. UPI is a system that powers multiple bank accounts (of participating banks), several banking services features like fund transfer, and merchant payments in a single mobile application. UPI or unified payment interface is a payment mode which is used to make fund transfers through the mobile app. User can transfer funds between two accounts using UPI apps. User must register for mobile banking to use UPI apps. Currently, this service is only available for android phone users. User need to download a UPI app and create a VPA or UPI ID. There are too many good UPI apps available such as BHIM, SBI UPI app, HDFC UPI app, iMobile, PhonePe app etc. as shown in the Fig. 4.7.1.

Fig. 4.7.1: UPI Apps

(ii) **Immediate Payment Service (IMPS):** It is an instant interbank electronic fund transfer service through mobile phones. It is also being extended through other channels such as ATM, Internet Banking etc.

(iii) **Mobile Apps: BHIM (Bharat Interface for Money)** is a Mobile App developed by National Payments Corporation of India (NPCI) based on UPI (Unified Payment Interface). It facilitates e-payments directly through banks and supports all Indian banks which use that platform. It is built on the Immediate Payment Service infrastructure and allows the user to instantly transfer money between the bank accounts of any two parties. BHIM works on all mobile devices and enables users to send or receive money to other UPI payment addresses by scanning QR code or using account number with Indian Financial Systems Code (IFSC) code or MMID (Mobile Money Identifier) Code for users who do not have a UPI-based bank account.

(iv) **Mobile Wallets:** It is defined as virtual wallets that stores payment card information on a mobile device. Mobile Wallets provide a convenient way for a user to make-in-store payments and can be used that merchants listed with the mobile wallet service providers. There are mobile wallets like Paytm, Freecharge, Buddy, Mobikwik etc. Some of these are owned by banks and some are owned by private companies.

(v) **Aadhar Enabled Payment Service(AEPS):** Government of India, is planning to launch this in near future. AEPS is an Aadhaar based digital payment mode. Customer needs only his or her Aadhaar number to pay to any merchant. AEPS allows bank to bank transactions. It means the money you pay will be deducted from your account and credited to the payee's account directly. Customers will need to link their AADHAR numbers to their bank accounts. APES once launched can be used at POS terminals also.

(vi) **Unstructured Supplementary Service Data(USSD):** A revolutionary idea, where to make payments through mobiles there is neither need for internet nor any smart phone. USSD banking or *99# Banking is a mobile banking based digital payment mode. User does not need to have a smartphone or internet connection to use USSD banking. S/he can easily use it with any normal feature phone. USSD banking is as easy as checking of mobile balance. S/he can use this service for many financial and non-financial operations such as checking balance, sending money, changing Mobile Banking Personal Identification number (MPIN) and getting Mobile Money Identifier (MMID).

II. Traditional Methods of Digital Payment

(i) **E-Wallet:** E-wallet or mobile wallet is the digital version of physical wallet with more functionality. User can keep his / her money in an E-wallet and use it when needed. Use the E-wallets to recharge phone, pay at various places and send money to friends. If user's have a smartphone and a stable internet connection, they can use E-wallets to make payments. These E-Wallets also give additional cashback offers. Some of the most used E-wallets are State bank buddy, ICICI Pockets, Freecharge, Paytm etc. as shown in the Fig. 4.7.2.

Fig. 4.7.2: E-Wallets

(ii) **Cards:** Cards are provided by banks to their account holders. These have been the most used digital payment modes till now. Various types of cards are as follows:

- **Credit Cards:** A small plastic card issued by a bank, or issuer etc., allowing the holder to purchase goods or services on credit. In this mode of payment, the buyer's cash flow is not immediately impacted. User of the card makes payment to card issuer at end of billing cycle which is generally a monthly cycle. Credit Card issuer charge customers per transactions / 5% of transaction as transaction fees.

- **Debits Cards:** A small plastic card issued by a bank. Allowing the holder to purchase goods or services on credit. In this mode of payment, the buyer's cash flow is immediately affected that as soon as payment is authorized buyers account is debited.

(iii) **Net Banking:** In this mode, the customers log to his / her bank account and makes payments. All public sectors, large private sector banks allow net banking facilities to their customers.

4.7.2 Advantages of Digital Payments

(i) **Easy and convenient:** Digital payments are easy and convenient. Person do not need to take loads of cash with themselves.

(ii) **Pay or send money from anywhere:** With digital payment modes, one can pay from anywhere anytime.

(iii) **Discounts from taxes:** Government has announced many discounts to encourage digital payments. User get 0.75% discounts on fuels and 10% discount on insurance premiums of government insurers.

(iv) **Written record:** User often forgets to note down his / her spending, or even if nothing is done it takes a lot of time. These are automatically recorded in passbook or inside E-Wallet app. This helps to maintain record, track spending and budget planning.

(v) **Less Risk:** Digital payments have less risk if used wisely. If user losses mobile phone or debit/credit card or Aadhar card, no need to worry a lot. No one can use anyone else's money without MPIN, PIN or fingerprint in the case of Aadhar. It is advised that user should get card blocked, if lost.

4.7.3 Drawbacks of Digital Payments

Every coin has two sides so as the digital payments. Despite many advantages, digital payments have a few drawbacks also.

(i) **Difficult for a Non-technical person:** As most of the digital payment modes are based on mobile phone, the internet and cards. These modes are somewhat difficult for non-technical persons such as farmers, workers etc.

(ii) **The risk of data theft:** There is a big risk of data theft associated with the digital payment. Hackers can hack the servers of the bank or the E-Wallet a customer is using and easily get his/her personal information. They can use this information to steal money from the customer's account.

(iii) **Overspending:** One keeps limited cash in his/her physical wallet and hence thinks twice before buying anything. But if digital payment modes are used, one has an access to all his/her money that can result in overspending.

4.8 COMPUTING TECHNOLOGIES

Recently, emerging technologies are seen to be having enormous potential to meet the global challenges. One of the high-potential technologies is informatics. It is expected to revolutionize the value-additions to the huge information component, which is growing exponentially. Technological innovations in the field of storage, mining and services may be the key to address emerging challenges. Though several other advance technologies include synthetic biology, Nano-scale design, systems biology, wireless networks, Information and Communications Technology (ICT) enhanced educational systems etc.; ICT appears to be spearheading all such developments at one or the other levels. To add some flavor to address the challenges, some of the technologies, which have recently emerged and are being rapidly adapted include cloud, grid, mobile, and green computing.

4.8.1 Virtualization

In computing, **Virtualization** means to create a virtual version of a device or resource, such as a server, storage device, network or even an operating system where the framework divides the resource into one or more execution environments. Virtualization refers to technologies designed to provide a layer of abstraction between computer hardware systems and the software running on them. By providing a logical view of computing resources, rather than a physical view; virtualization allows its' users to manipulate their systems' operating systems into thinking that a group of servers is a single pool of computing resources and conversely, allows its users to run multiple operating systems simultaneously on a single machine.

I. Concept of Virtualization

The core concept of Virtualization lies in Partitioning, which divides a single physical server into multiple logical servers. Once the physical server is divided, each logical server can run an operating system and applications independently. For example - Partitioning of a hard drive is considered virtualization because one drive is partitioned in a way to create two separate hard drives. Devices, applications and human users are able to interact with the virtual resource as if it were a real single logical resource.

II. Application Areas of Virtualization

- **Server Consolidation:** Virtual machines are used to consolidate many physical servers into fewer servers, which in turn host virtual machines. Each physical server is reflected as a virtual machine "guest" residing on a virtual machine host system. This is also known as "Physical-to-Virtual" or 'P2V' transformation.
- **Disaster Recovery:** Virtual machines can be used as "hot standby" environments for physical production servers. This changes the classical "backup-and-restore" philosophy, by providing backup images that can "boot" into live virtual machines, capable of taking over workload for a production server experiencing an outage.
- **Testing and Training:** Virtualization can give root access to a virtual machine. This can be very useful such as in kernel development and operating system courses.
- **Portable Applications:** Portable applications are needed when running an application from a removable drive, without installing it on the system's main disk drive. Virtualization can be used to encapsulate the application with a redirection layer that stores temporary files, windows registry entries and other state information in the application's installation directory and not within the system's permanent file system.
- **Portable Workspaces:** Recent technologies have used virtualization to create portable workspaces on devices like iPods and USB memory sticks.

III. Common Types of Virtualization

- **Hardware Virtualization:** Hardware Virtualization or Platform Virtualization refers to the creation of a virtual machine that acts like a real computer with an operating system. Software executed on these virtual machines is separated from the underlying hardware resources. For example, a computer that is running Microsoft Windows may host a virtual machine that looks like a computer with the Linux operating system; based software that can be run on the virtual machine.

  The basic idea of Hardware virtualization is to consolidate many small physical servers into one large physical server so that the processor can be used more effectively. The software that creates a virtual machine on the host hardware is called a hypervisor or Virtual Machine Manager. The hypervisor controls the processor, memory and other components by allowing several different operating systems to run on the same machine without the need for a source code. The operating system running on the machine will appear to have its own processor, memory and other components.

♦ **Network Virtualization: Network Virtualization** is a method of combining the available resources in a network by splitting up the available bandwidth into channels, each of which is independent from the others, and each of which can be assigned (or reassigned) to a particular server or device in real time. This allows a large physical network to be provisioned into multiple smaller logical networks and conversely allows multiple physical LANs to be combined into a larger logical network. This behavior allows administrators to improve network traffic control, enterprise and security. Network virtualization involves platform virtualization, often combined with resource virtualization.

  Various equipment and software vendors offer network virtualization by combining any of the Network hardware such as switches and Network Interface Cards (NICs); Network elements such as firewalls and load balancers; Networks such as virtual LANs (VLANs); Network storage devices; Network machine-to-machine elements such as telecommunications devices; Network mobile elements such as laptop computers, tablet computers, smart phones and Network media such as Ethernet and Fiber Channel. Network virtualization is intended to optimize network speed, reliability, flexibility, scalability, and security.

♦ **Storage Virtualization: Storage Virtualization** is the apparent pooling of data from multiple storage devices, even different types of storage devices, into what appears to be a single device that is managed from a central console. Storage virtualization helps the storage administrator perform the tasks of backup, archiving, and recovery more easily and in less time by disguising the actual complexity of a Storage Area Network (SAN). Administrators can implement virtualization with software applications or by using hardware and software hybrid appliances. The servers connected to the storage system aren't aware of where the data really is. Storage virtualization is sometimes described as "abstracting the logical storage from the physical storage.

4.8.2 Grid Computing

The computing resources in most of the organizations are underutilized but are necessary for certain operations. The idea of Grid computing is to make use of such non-utilized computing power by the needy organizations, and thereby the Return on Investment (RoI) on computing investments can be increased.

Grid Computing is a computer network in which each computer's resources are shared with every other computer in the system. It is a distributed architecture of large numbers of computers connected to solve a complex problem. In the grid computing model, servers or personal computers run independent tasks and are loosely linked by the Internet or low-speed networks. A typical Grid Model is shown in Fig. 4.8.1.

It is a special kind of distributed computing. In distributed computing, different computers within the same network share one or more resources. In the ideal grid computing system, every resource is shared, turning a computer network into a powerful supercomputer. With the right user interface, accessing a grid computing system would look no different than accessing a local machine's resources. Every authorized computer would have access to enormous processing power and storage capacity.

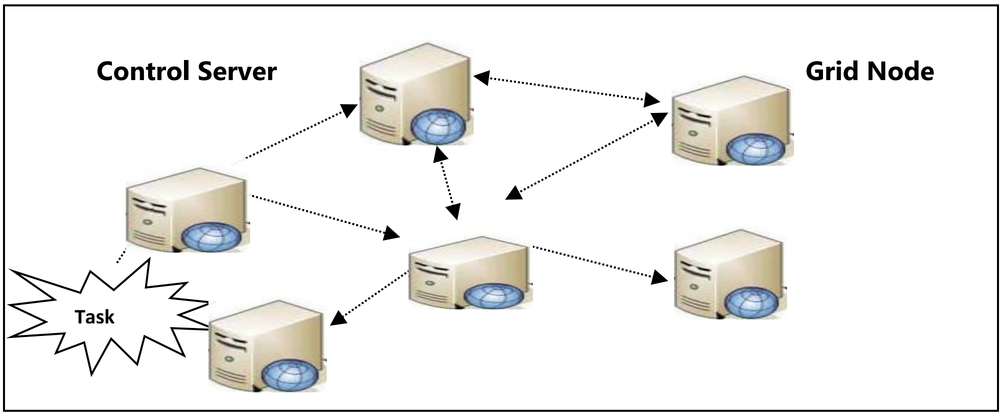


Fig. 4.8.1: Grid Computing Scenario

I. Benefits of Grid Computing

- **Making use of Underutilized Resources:** In most organizations, there are large amounts of underutilized computing resources including even the server machines. Grid computing provides a framework for exploiting these underutilized resources and thus has the possibility of substantially increasing the efficiency of resource usage. Grid computing (more specifically, a data grid) can be used to aggregate this unused storage into a much larger virtual data store, possibly configured to achieve improved performance and reliability over that of any single machine.

- **Resource Balancing:** For applications that are grid-enabled, the grid can offer a resource balancing effect by scheduling grid jobs on machines with low utilization. This feature of grid computing handles occasional peak loads of activity in parts of a larger organization. An unexpected peak can be routed to relatively idle machines in the grid; and if the grid is already fully utilized, the lowest priority work being performed on the grid can be temporarily suspended or even cancelled and performed again later to make room for the higher priority work.
- **Parallel CPU Capacity:** The potential for usage of massive parallel CPU capacity is one of the most common visions and attractive features of a grid. A CPU-intensive grid application can be thought of as many smaller sub-jobs, each executing on a different machine in the grid. To the extent that these sub-jobs do not need to communicate with each other, the more scalable the application becomes. A perfectly scalable application will, for example, finish in one tenth of the time if it uses ten times the number of processors.
- **Virtual resources and virtual organizations for collaboration:** Grid computing provides an environment for collaboration among a wider audience. The users of the grid can be organized dynamically into several virtual organizations, each with different policy requirements. These virtual organizations can share their resources such as data, specialized devices, software, services, licenses, and so on, collectively as a larger grid. The grid can help in enforcing security rules among them and implement policies, which can resolve priorities for both resources and users.
- **Access to additional resources:** In addition to CPU and storage resources, a grid can provide access to other resources as well. For example, if a user needs to increase their total bandwidth to the Internet to implement a data mining search engine, the work can be split among grid machines that have independent connections to the Internet. In this way, total searching capability is multiplied, since each machine has a separate connection to the Internet.
- **Reliability:** High-end conventional computing systems use expensive hardware to increase reliability. The machines also use duplicate

processors in such a way that when they fail, one can be replaced without turning the other off. Power supplies and cooling systems are duplicated. The systems are operated on special power sources that can start generators if utility power is interrupted. All of this builds a reliable system, but at a great cost, due to the duplication of expensive components.

- ♦ **Management:** The goal to virtualize the resources on the grid and more uniformly handle heterogeneous systems create new opportunities to better manage a larger, more distributed IT infrastructure. The grid offers management of priorities among different projects. Aggregating utilization data over a larger set of projects can enhance an organization's ability to project future upgrade needs. When maintenance is required, grid work can be rerouted to other machines without crippling the projects involved.

II. Types of Resources

A grid is a collection of machines, sometimes referred to as nodes, resources, members, donors, clients, hosts and many other such terms. They all contribute any combination of resources to the grid as a whole. Some resources may be used by all users of the grid, while others may have specific restrictions.

- ♦ **Computation:** The most common resource is Computing Cycles provided by the processors of the machines on the grid where processors can vary in speed, architecture, software platform, and other associated factors such as memory, storage, and connectivity. There are three primary ways to exploit the computation resources of a grid.
    - o To run an existing application on an available machine on the grid rather than locally;
    - o To use an application designed to split its work in such a way that the separate parts can execute in parallel on different processors; and
    - o To run an application, that needs to be executed many times, on many different machines in the grid.
- ♦ **Storage:** The second most common resource used in a grid is Data Storage. A grid providing an integrated view of data storage is sometimes called a Data Grid. Each machine on the grid usually provides some quantity of storage for grid use, even if temporary. Storage can be memory attached to the processor or it can be

secondary storage, using hard disk drives or other permanent storage media. More advanced file systems on a grid can automatically duplicate sets of data, to provide redundancy for increased reliability and increased performance.

- **Communications:** Communications within the grid are important for sending jobs and their required data to points within the grid. The bandwidth available for such communications can often be a critical resource that can limit utilization of the grid. Redundant communication paths are sometimes needed to better handle potential network failures and excessive data traffic. In some cases, higher speed networks must be provided to meet the demands of jobs transferring larger amounts of data.
- **Software and Licenses:** The grid may have software installed that may be too expensive to install on every grid machine. Some software licensing arrangements permit the software to be installed on all of the machines of a grid but may limit the number of installations that can be simultaneously used at any given instant. License management software keeps track of how many concurrent copies of the software are being used and prevents more than that number from executing at any given time.
- **Special equipment, capacities, architectures, and policies:** Platforms on the grid will often have different architectures, operating systems, devices, capacities, and equipment. Each of these items represents a different kind of resource that the grid can use as criteria for assigning jobs to machines. For example, some machines may be designated to only be used for medical research. These would be identified as having a medical research attribute and the scheduler could be configured to only assign jobs that require machines of the medical research resource.

III. Application Areas of Grid Computing

- Civil engineers collaborate to design, execute, & analyze shake table experiments.
- An insurance company mines data from partner hospitals for fraud detection.
- An application service provider offloads excess load to a compute cycle provider.

- An enterprise configures internal & external resources to support e-Business workload.
- Large-scale science and engineering are done through the interaction of people, heterogeneous computing resources, information systems and instruments, all of which are geographically and organizationally dispersed.

IV. Grid Computing Security

To develop security architecture, following constraints are taken from the characteristics of grid environment and application.

- **Single Sign-on:** A user should authenticate once and they should be able to acquire resources, use them, and release them and to communicate internally without any further authentication.
- **Protection of Credentials:** User passwords, private keys, etc. should be protected.
- **Interoperability with local security solutions:** Access to local resources should have local security policy at a local level. Despite of modifying every local resource there is an inter-domain security server for providing security to local resource.
- **Exportability:** The code should be exportable i.e. they cannot use a large amount of encryption at a time. There should be a minimum communication at a time.
- **Support for secure group communication:** In a communication, there are number of processes which coordinate their activities. This coordination must be secure and for this there is no such security policy.
- **Support for multiple implementations:** There should be a security policy which should provide security to multiple sources based on public and private key cryptography.

4.8.3 Cloud Computing

To understand Cloud Computing, we first must understand what the cloud is. **"The Cloud"** refers to applications, services, and data storage on the Internet. These service providers rely on giant server farms and massive storage devices that are connected via Internet protocols. Cloud Computing is the use of these services by individuals and organizations. You probably already use cloud computing in some forms. For example, if you access your e-mail via your web browser, you are using a form of cloud computing. If you use Google Drive's applications, you are using cloud computing. While these are free versions of cloud computing, there is big business in providing applications and data storage over the web. Salesforce is a good example of cloud computing as their entire suite of CRM applications are offered via the cloud. Cloud Computing is not limited to web applications; it can also be used for services such as phone or video streaming. The best example of Cloud Computing is Google Apps where any application can be accessed using a browser and it can be deployed on thousands of computers through the Internet.

Cloud Computing, simply means the use of computing resources as a service through networks, typically the Internet. The Internet is commonly visualized as clouds; hence the term "cloud computing" for computation done through the Internet. With Cloud Computing, users can access database resources via the Internet from anywhere, for as long as they need, without worrying about any maintenance or management of actual resources. Besides these, databases in cloud may be highly dynamic and scalable. In fact, it is a very independent platform in terms of computing.

Cloud Computing is both, a combination of software and hardware based computing resources delivered as a networked service. This model of IT enabled services enables anytime access to a shared pool of applications and resources. These applications and resources can be accessed using a simple front-end interface such as a Web browser, and thus enabling users to access the resources from any client device including notebooks, desktops and mobile devices.

Cloud Computing provides the facility to access shared resources and common infrastructure offering services on demand over the network to perform operations that meet changing business needs (shown in Fig. 4.8.2). The location of physical resources and devices being accessed are typically not known to the end user. It also provides facilities for users to develop, deploy and manage their applications 'on the cloud', which entails virtualization of resources that maintains and manages itself.

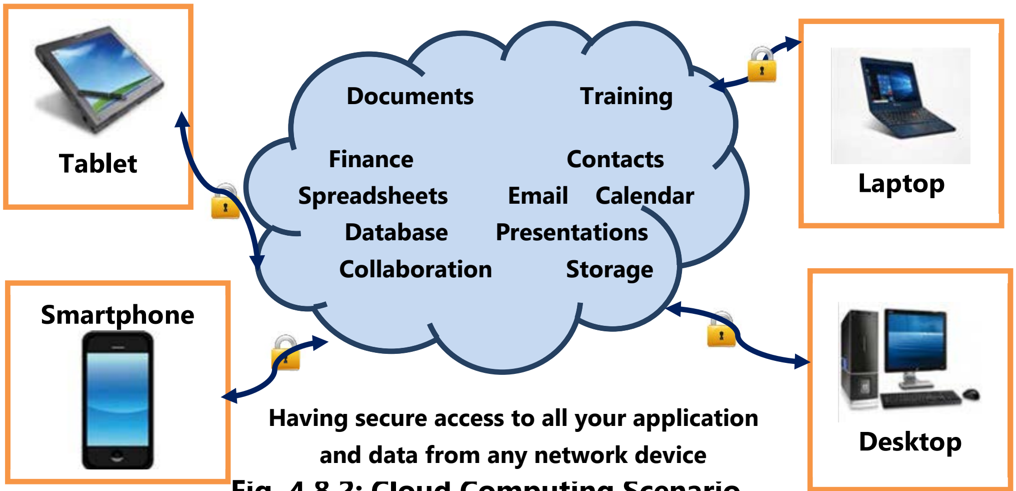


Fig. 4.8.2: Cloud Computing Scenario

With cloud computing, companies can scale up to massive capacities in an instant without having to invest in new infrastructure, train new personnel or license new software. Cloud computing is of benefit to small and medium-sized business systems, who wish to completely outsource their data-center infrastructure; or large companies, who wish to get peak load capacity without incurring the higher cost of building larger data centers internally. In both the instances, service consumers use **'what they need on the Internet'** and **'pay only for what they use'**.

The service consumer may no longer be required to pay for a PC, use an application from the PC, or purchase a specific software version that's configured for smart phones, PDAs, and other devices. The consumers may not own the infrastructure, software, or platform in the cloud based schemes, leading to lower up-fronts, capital, and operating expenses. End users may not need to care about how servers and networks are maintained in the cloud, and can access multiple servers anywhere on the globe without knowing 'which ones and where they are located'.

I. Characteristics of Cloud Computing

The following is a list of characteristics of a cloud-computing environment. Not all characteristics may be present in a specific cloud solution. However, some of the key characteristics are given as follows:

- **Elasticity and Scalability:** Cloud computing gives us the ability to expand and reduce resources according to the specific service requirement. For example, we may need a large number of server resources for the duration of a specific task. We can then release these server resources after we complete our task.
- **Pay-per-Use:** We pay for cloud services only when we use them, either for the short term (for example, for CPU time) or for a longer duration (for example, for cloud-based storage or vault services).
- **On-demand:** Because we invoke cloud services only when we need them, they are not permanent parts of the IT infrastructure. This is a significant advantage for cloud use as opposed to internal IT services. With cloud services, there is no need to have dedicated resources waiting to be used, as is the case with internal services.
- **Resiliency:** The resiliency of a cloud service offering can completely isolate the failure of server and storage resources from cloud users. Work is migrated to a different physical resource in the cloud with or without user awareness and intervention.

- **Multi Tenancy:** Public cloud service providers often can host the cloud services for multiple users within the same infrastructure. Server and storage isolation may be physical or virtual depending upon the specific user requirements.
- **Workload Movement:** This characteristic is related to resiliency and cost considerations. Here, cloud-computing providers can migrate workloads across servers both inside the data center and across data centers (even in a different geographic area). This migration might be necessitated by cost (less expensive to run a workload in a data center in another country based on time of day or power requirements) or efficiency considerations (for example, network bandwidth). A third reason could be regulatory considerations for certain types of workloads.

II. Advantages of Cloud Computing

- **Achieve economies of scale:** Volume output or productivity can be increased even with fewer systems and thereby reduce the cost per unit of a project or product.
- **Reduce spending on technology infrastructure:** Data and information can be accessed with minimal upfront spending in a pay-as-you-go approach, which is based on demand.
- **Globalize the workforce:** People worldwide can access the cloud with Internet connection.
- **Streamline business processes:** Getting more work done in less time with less resources are possible.
- **Reduce capital costs:** Not required to spend huge money on hardware, software, or licensing fees.
- **Pervasive accessibility:** Data and applications can be accesses anytime, anywhere, using any smart computing device, making our life so much easier.
- **Monitor projects more effectively:** It is feasible to confine within budgetary allocations and can be ahead of completion cycle times.
- **Less personnel training is needed:** It takes fewer people to do more work on a cloud, with a minimal learning curve on hardware and software issues.

- **Minimize maintenance and licensing software:** As there is no too much of non-premise computing resources, maintenance becomes simple and updates and renewals of software systems rely on the cloud vendor or provider.
- **Improved flexibility:** It is possible to make fast changes in our work environment without serious issues at stake.

III. Drawbacks of Cloud Computing

- If Internet connection is lost, the link to the cloud and thereby to the data and applications is lost.
- Security is a major concern as entire working with data and applications depend on other cloud vendors or providers.
- Although Cloud computing supports scalability (ie. quickly scaling up and down computing resources depending on the need), it does not permit the control on these resources as these are not owned by the user or customer.
- Depending on the cloud vendor or provide, customers may have to face restrictions on the availability of applications, operating systems and infrastructure options.
- Interoperability (ability of two or more applications that are required to support a business need to work together by sharing data and other business-related resources) is an issue wherein all the applications may not reside with a single cloud vendor and two vendors may have applications that do not cooperate with each other.

IV. Cloud Computing Environment

The Cloud Computing environment can consist of multiple types of clouds based on their deployment and usage. Such typical Cloud computing environments, catering to special requirements, are briefly described as follows (given in Fig. 4.8.3).

(A) Private Cloud: This cloud computing environment resides within the boundaries of an organization and is used exclusively for the organization's benefits. These are also called **Internal Clouds** or Corporate Clouds. Private Clouds can either be private to the organization and managed by the single organization **(On-Premise Private Cloud)** or can be managed by third party **(Outsourced Private Cloud)**. They are built primarily by IT departments within enterprises, who seek to optimize utilization of infrastructure resources within the enterprise by provisioning the infrastructure with applications using the concepts of grid and virtualization.

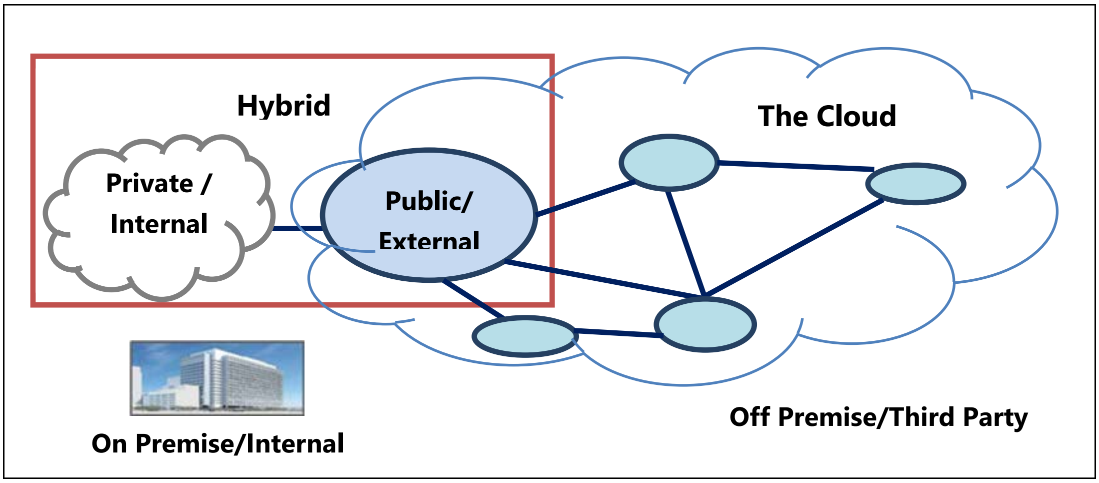


Fig. 4.8.3: Cloud Deployment Models

Characteristics of Private Cloud

- **Secure:** The private cloud is secure as it is deployed and managed by the organization itself, and hence there is least chance of data being leaked out of the cloud.
- **Central Control:** As usually the private cloud is managed by the organization itself, there is no need for the organization to rely on anybody and its controlled by the organization itself.
- **Weak Service Level Agreements (SLAs):** SLAs play a very important role in any cloud service deployment model as they are defined as agreements between the user and the service provider in private cloud. In private cloud, either Formal SLAs do not exist or are weak as it is between the organization and user of the same organization. Thus, high availability and good service may or may not be available.

Advantages of Private Cloud

- It improves average server utilization; allow usage of low-cost servers and hardware while providing higher efficiencies; thus, reducing the costs that a greater number of servers would otherwise entail.
- It provides a high level of security and privacy to the user.
- It is small and controlled and maintained by the organization.

Moreover, one major **limitation of Private Cloud** is that IT teams in the organization may have to invest in buying, building and managing the clouds independently. Budget is a constraint in private clouds and they also have loose SLAs.

(B) Public Cloud: The public cloud is the cloud infrastructure that is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organizations, or some combination of them. Typically, public clouds are administrated by third parties or vendors over the Internet, and the services are offered on pay-per-use basis. These are also called Provider Clouds. Public cloud consists of users from all over the world wherein a user can simply purchase resources on an hourly basis and work with the resources which are available in the cloud provider's premises.

Characteristics of Public Cloud

- **Highly Scalable:** The resources in the public cloud are large in number and the service providers make sure that all requests are granted. Hence public clouds are scalable.
- **Affordable:** The cloud is offered to the public on a pay-as-you-go basis; hence the user has to pay only for what he or she is using (using on a per-hour basis). And this does not involve any cost related to the deployment.
- **Less Secure:** Since it is offered by a third party and they have full control over the cloud, the public cloud is less secure out of all the other deployment models.
- **Highly Available:** It is highly available because anybody from any part of the world can access the public cloud with proper permission, and this is not possible in other models as geographical or other access restrictions might be there.
- **Stringent SLAs:** As the service provider's business reputation and customer strength are totally dependent on the cloud services, they follow the SLAs strictly and violations are avoided.

Advantages of Public Cloud

- It is widely used in the development, deployment and management of enterprise applications, at affordable costs.

- It allows the organizations to deliver highly scalable and reliable applications rapidly and at more affordable costs.
- There is no need for establishing infrastructure for setting up and maintaining the cloud.
- Strict SLAs are followed.
- There is no limit for the number of users.

Moreover, one of the **limitation of Public cloud** is security assurance and thereby building trust among the clients is far from desired but slowly liable to happen. Further, privacy and organizational autonomy are not possible.

(C) **Hybrid Cloud:** This is a combination of both at least one private (internal) and at least one public (external) cloud computing environments - usually, consisting of infrastructure, platforms and applications. The usual method of using the hybrid cloud is to have a private cloud initially, and then for additional resources, the public cloud is used. The hybrid cloud can be regarded as a private cloud extended to the public cloud and aims at utilizing the power of the public cloud by retaining the properties of the private cloud. It is typically offered in either of two ways. A vendor has a private cloud and forms a partnership with a public cloud provider or a public cloud provider forms a partnership/franchise with a vendor that provides private cloud platforms. Fig. 4.8.4 depicts Hybrid Cloud.

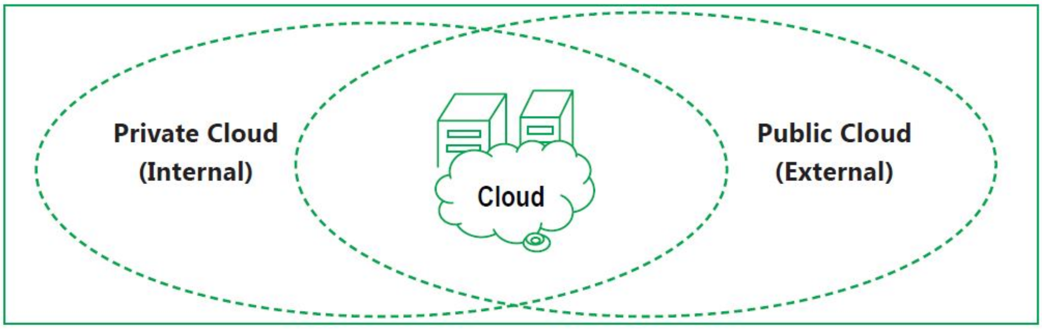


Fig. 4.8.4: Hybrid Cloud

Characteristics of Hybrid Cloud

- **Scalable:** The hybrid cloud has the property of public cloud with a private cloud environment and as the public cloud is scalable; the hybrid cloud with the help of its public counterpart is also scalable.

- **Partially Secure:** The private cloud is considered as secured and public cloud has high risk of security breach. The hybrid cloud thus cannot be fully termed as secure but as partially secure.
- **Stringent SLAs:** Overall the SLAs are more stringent than the private cloud and might be as per the public cloud service providers.
- **Complex Cloud Management:** Cloud management is complex as it involves more than one type of deployment models and the number of users is high.

The **Advantages of Hybrid Cloud** include the following:

- It is highly scalable and gives the power of both private and public clouds.
- It provides better security than the public cloud.

The **limitation of Hybrid Cloud** is that the security features are not as good as the private cloud and complex to manage.

(D) Community Cloud: The community cloud is the cloud infrastructure that is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (eg. mission security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party or some combination of them, and it may exist on or off premises. In this, a private cloud is shared between several organizations. Fig. 4.8.5 depicts Community Cloud. This model is suitable for organizations that cannot afford a private cloud and cannot rely on the public cloud either.

Characteristics of Community Cloud

- **Collaborative and Distributive Maintenance:** In this, no single company has full control over the whole cloud. This is usually distributive and hence better cooperation provides better results.
- **Partially Secure:** This refers to the property of the community cloud where few organizations share the cloud, so there is a possibility that the data can be leaked from one organization to another, though it is safe from the external world.
- **Cost Effective:** As the complete cloud if being shared by several organizations or community, not only the responsibility gets shared; the community cloud becomes cost effective too.

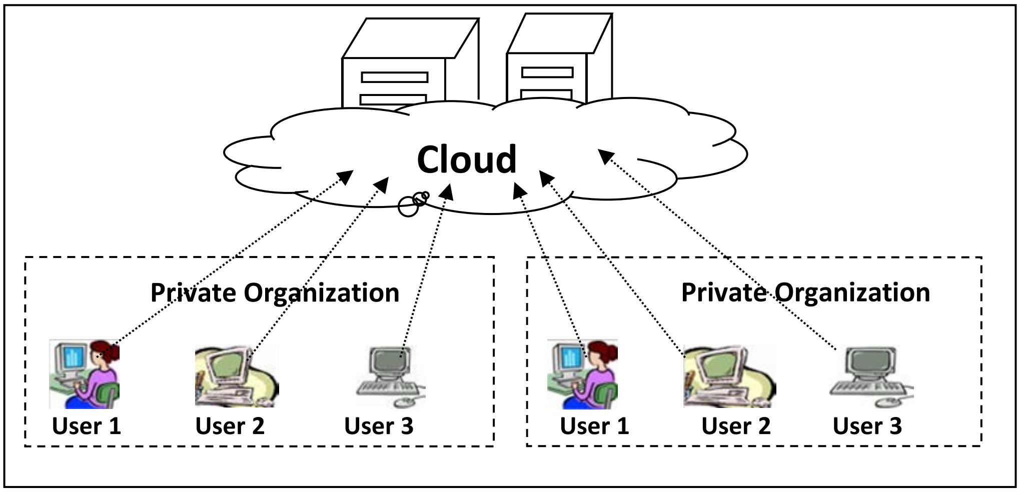


Fig. 4.8.5: Community Cloud

Advantages of Community Cloud

- It allows establishing a low-cost private cloud.
- It allows collaborative work on the cloud.
- It allows sharing of responsibilities among the organizations.
- It has better security than the public cloud.

The **limitation of the Community Cloud** is that the autonomy of the organization is lost and some of the security features are not as good as the private cloud. It is not suitable in the cases where there is no collaboration.

V. Cloud Computing Service Models

Cloud computing is a model that enables the end users to access the shared pool of resources such as compute, network, storage, database and application as an on-demand service without the need to buy or own it. The services are provided and managed by the service provider, reducing the management effort from the end user side. The essential characteristics of the cloud include on-demand, self-service, broad network access, resource pooling, rapid elasticity, and measured service. The National Institute of Standards and Technology (NIST) defines three basic service models - Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These are pictorially presented in Fig. 4.8.6.

(A) Infrastructure as a Service (IaaS): IaaS, a hardware-level service, provides computing resources such as processing power, memory, storage, and networks for cloud users to run their application on-demand. This allows users to maximize the utilization of computing capacities without having to own and manage their own resources. The end-users or IT architects will use the infrastructure resources in the form of Virtual machines (VMs) and design virtual infrastructure, network load balancers etc., based on their needs. The IT architects need not maintain the physical servers as it is maintained by the service providers. Examples of IaaS providers include Amazon Web Services (AWS), Google Compute Engine, OpenStack and Eucalyptus.

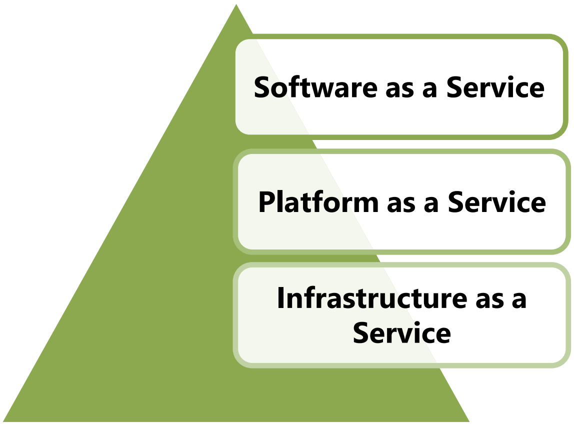


Fig. 4.8.6: Cloud Computing Basic Service Models

(i) Characteristics of IaaS

- **Web access to the resources:** The IaaS model enables the IT users to access infrastructure resources over the Internet. When accessing a huge computing power, the IT user need not get physical access to the servers.
- **Centralized Management:** The resources distributed across different parts are controlled from any management console that ensures effective resource management and effective resource utilization.
- **Elasticity and Dynamic Scaling:** Depending on the load, IaaS services can provide the resources and elastic services where the usage of resources can be increased or decreased according to the requirements.
- **Shared infrastructure:** IaaS follows a one-to-many delivery model and allows multiple IT users to share the same physical infrastructure and thus ensure high resource utilization.

- **Metered Services:** IaaS allows the IT users to rent the computing resources instead of buying it. The services consumed by the IT user will be measured, and the users will be charged by the IaaS providers based on the amount of usage.

(ii) Different instances of IaaS (as discussed in the Table 4.8.1)

Table 4.8.1: Instances of IaaS

Instance	Description
Network as a Service (NaaS)	• Provides users with needed data communication capacity to accommodate bursts in data traffic during data-intensive activities such as video conferencing or large file downloads. • It is an ability given to the end-users to access virtual network services that are provided by the service provider over the Internet on a per-per-use basis. • Allows network architects to create virtual networks; virtual network interface cards (NICs), virtual routers, virtual switches, and other networking components. • Allows the network architect to deploy custom routing protocols and enables the design of efficient in-network services, such as data aggregation, stream processing, and caching. NaaS providers operate using three common service models: Virtual Private Network (VPN), Bandwidth on Demand (BoD) and Mobile Virtual Network (MVN).
Storage as a Service (STaaS)	• Provides storage infrastructure on a subscription basis to users who want a low-cost and convenient way to store data, synchronize data across multiple devices, manage off-site backups, mitigate risks of disaster recovery, and preserve records for the long-term. • It is an ability given to the end users to store the data on the storage services provided by the service provider. • STaaS allows the end users to access the files at any time from any place. STaaS provider provides the virtual storage that is abstracted from the physical storage of any cloud data center.
Database as a Service (DBaaS)	• Provides users with seamless mechanisms to create, store, and access databases at a host site on demand. • It is an ability given to the end users to access the database service without the need to install and maintain it on the pay-per-use basis.

	• The end users can access the database services through any Application Programming Interfaces (APIs) or Web User Interfaces provided by the service provider.
Backend as a Service (BaaS)	• Provides web and mobile app developers a way to connect their applications to backend cloud storage with added services such as user management, push notifications, social network services integration using custom software development kits and application programming interfaces.
Desktop as a Service (DTaaS)	• Provides ability to the end users to use desktop virtualization without buying and managing their own infrastructure. • It is a pay-per-use cloud service delivery model in which the service provider manages the back-end responsibilities of data storage, backup, security and upgrades. • The end-users are responsible for securing for managing their own desktop images, applications, and security. These services are simple to deploy, are highly secure, and produce better experience on almost all devices.

(B) **Platform as a Service (PaaS): PaaS** provides the users the ability to develop and deploy an application on the development platform provided by the service provider. In traditional application development, the application will be developed locally and will be hosted in the central location. In stand-alone application development, the application will be developed by traditional development platforms result in licensing - based software, whereas PaaS changes the application development from local machine to online. For example - Google App Engine, Windows Azure Compute etc.

Typical PaaS providers may provide programming languages, application frameworks, databases, and testing tools apart from some build tools, deployment tools and software load balancers as a service in some cases.

(C) **Software as a Service (SaaS): SaaS** provides ability to the end users to access an application over the Internet that is hosted and managed by the service provider. Thus, the end users are exempted from managing or controlling an application the development platform, and the underlying infrastructure. SaaS changes the way the software is delivered to the customers. SaaS provides users to access large variety of applications over internets that are hosted on service provider's infrastructure. For example, one can make his/her own word document in Google docs online, s/he can edit a photo online on pixlr.com so s/he need not install the photo editing software on his/her system - thus Google is provisioning software as a service. Different instances of SaaS are discussed in the Table 4.8.2.

Table 4.8.2: Instances of SaaS

Instance	**Description**
Testing as a Service (TaaS)	Provides users with software testing capabilities such as generation of test data, generation of test cases, execution of test cases and test result evaluation on a pay-per-use basis.
API as a Service (APIaaS)	Allows users to explore functionality of Web services such as Google Maps, Payroll processing, and credit card processing services etc.
Email as a Service (EaaS)	Provides users with an integrated system of emailing, office automation, records management, migration, and integration services with archiving, spam blocking, malware protection, and compliance features.

(D) Other Cloud Service Models (Table 4.8.3)

Table 4.8.3: Other Cloud Service Models

Instance	**Description**
Communication as a Service (CaaS)	• It is an outsourced enterprise communication solution that can be leased from a single vender. The CaaS vendor is responsible for all hardware and software management and offers guaranteed Quality of Service (QoS). It allows businesses to selectively deploy communication devices and modes on a pay-as-you-go, as-needed basis. • This approach eliminates the large capital investments. Examples are: Voice over IP (VolP), Instant Messaging (IM), Collaboration and Videoconferencing application using fixed and mobile devices.
Data as a Service (DaaS)	• Provides data on demand to a diverse set of users, systems or application. The data may include text, images, sounds, and videos. • Data encryption and operating system authentication are commonly provided for security. DaaS users have access

	to high-quality data in a centralized place and pay by volume or data type, as needed. • However, as the data is owned by the providers, users can only perform read operations on the data. DaaS is highly used in geography data services and financial data services.
Security as a Service (SECaaS)	• It is an ability given to the end user to access the security service provided by the service provider on a pay-per-use basis. • It is a new approach to security in which cloud security is moved into the cloud itself whereby cloud service users will be protected from within the cloud using a unified approach to threats.
Identity as a Service (IDaaS)	• It is an ability given to the end users; typically, an organization or enterprise; to access the authentication infrastructure that is built, hosted, managed and provided by the third party service provider. • Generally, IDaaS includes directory services, authentication services, risk and event monitoring, single sign-on services, and identity and profile management.

4.8.4 Mobile Computing

Mobile Computing refers to the technology that allows transmission of data via a computer without having to be connected to a fixed physical link. Mobile voice communication is widely established throughout the world and has had a very rapid increase in the number of subscribers to the various cellular networks over the last few years. An extension of this technology is the ability to send and receive data across these cellular networks. This is the fundamental principle of mobile computing. Mobile data communication has become a very important and rapidly evolving technology as it allows users to transmit data from remote locations to other remote or fixed locations. This proves to be the solution of the biggest problem of business people on the move i.e. mobility. A primitive scenario of mobile computing in practice is given in the Fig. 4.8.7.

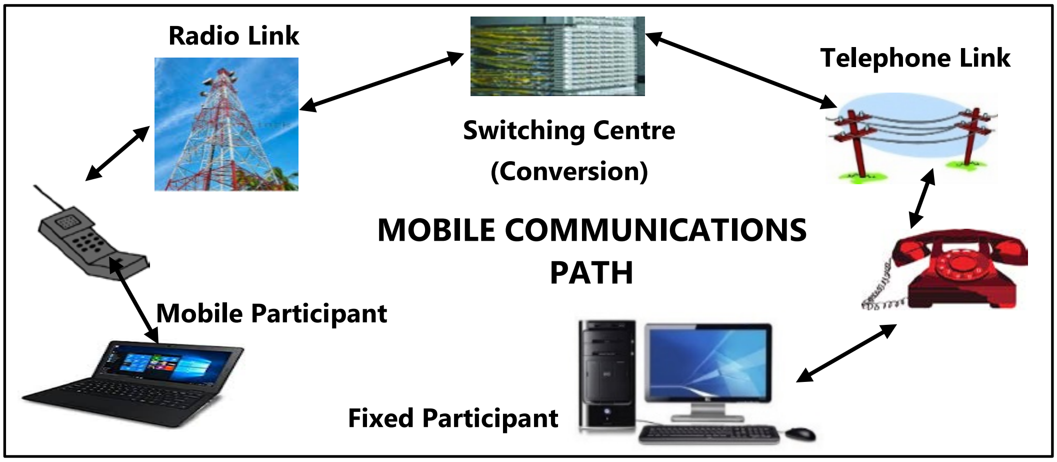


Fig. 4.8.7: Mobile Computing

I. Components of Mobile Computing

The key components of Mobile Computing are as follows:

- **Mobile Communication:** This refers to the infrastructure put in place to ensure that seamless and reliable communication goes on. This would include communication properties, protocols, data formats and concrete technologies.
- **Mobile Hardware:** Mobile Hardware includes mobile devices or device components that receive or access the service of mobility. They would range from Portable laptops, Smart Phones, Tablet PCs, and Personal Digital Assistants (PDA) that use an existing and established network to operate on. At the back end, there are various servers like Application Servers, Database Servers and Servers with wireless support, WAP gateway, a Communications Server and/or MCSS (Mobile Communications Server Switch) or a wireless gateway embedded in wireless carrier’s network. The characteristics of mobile computing hardware are defined by the size and form factor, weight, microprocessor, primary storage, secondary storage, screen size and type, means of input, means of output, battery life, communications capabilities, expandability and durability of the device.
- **Mobile Software:** Mobile Software is the actual programme that runs on the mobile hardware and deals with the characteristics and requirements of mobile applications. It is the operating system of that appliance and is the essential component that makes the mobile device operates. Mobile applications popularly called Apps are being

developed by organizations for use by customers but these apps could represent risks, in terms of flow of data as well as personal identification risks, introduction of malware and access to personal information of mobile owner.

II. Working of Mobile Computing

- The user enters or access data using the application on hand-held computing device.
- Using one of several connecting technologies, the new data are transmitted from hand-held to site's information system where files are updated and the new data are accessible to other system user.
- Now both systems (hand-held and site's computer) have the same information and are in sync.
- The process work the same way starting from the other direction.

The process is similar to the way a worker's desktop PC access the organization's applications, except that user's device is not physically connected to the organization's system. The communication between the user device and site's information systems uses different methods for transferring and synchronizing data, some involving the use of Radio Frequency (RF) technology.

III. Benefits of Mobile Computing

In general, Mobile Computing is a versatile and strategic technology that increases information quality and accessibility, enhances operational efficiency, and improves management effectiveness. But, more specifically, it leads to a range of tangible benefits, including the following:

- It provides mobile workforce with remote access to work order details, such as work order location, contact information, required completion date, asset history relevant warranties/service contracts.
- It enables mobile sales personnel to update work order status in real-time, facilitating excellent communication.
- It facilitates access to corporate services and information at any time, from anywhere.
- It provides remote access to the corporate Knowledge base at the job location.

- It enables to improve management effectiveness by enhancing information quality, information flow, and ability to control a mobile workforce.

IV. Limitations of Mobile Computing

- **Insufficient Bandwidth:** Mobile Internet access is generally slower than direct cable connections using technologies such as General Packet Radio Service (GPRS) and **E**nhanced **D**ata Rates for **G**SM (Global System for Mobile Communication) **E**volution - (EDGE), and 3G, 4G networks. These networks are usually available within range of commercial cell phone towers. Higher speed wireless LANs are inexpensive but have very limited range.

- **Security Standards:** When working mobile, one is dependent on public networks, requiring careful use of Virtual Private Network (VPN). Security is a major concern while concerning the mobile computing standards on the fleet. One can easily attack the VPN through a huge number of networks interconnected through the line.

- **Power consumption:** When a power outlet or portable generator is not available, mobile computers must rely entirely on battery power. Combined with the compact size of many mobile devices, this often means unusually expensive batteries must be used to obtain the necessary battery life. Mobile computing should also look into Greener IT in such a way that it saves the power or increases the battery life.

- **Transmission interferences:** Weather, terrain and the range from the nearest signal point can all interfere with signal reception. Reception in tunnels, some buildings, and rural areas is often poor.

- **Potential health hazards:** People who use mobile devices while driving is often distracted from driving, and are thus assumed more likely to be involved in traffic accidents. Cell phones may interfere with sensitive medical devices. There are allegations that cell phone signals may cause health problems.

- **Human interface with device:** Screens and keyboards tend to be small, which may make them hard to use. Alternate input methods such as speech or handwriting recognition require training.

4.8.5 Green Computing

Green Computing or **Green IT** refers to the study and practice of environmentally sustainable computing or IT. In other words, it is the study and practice of establishing/ using computers and IT resources in a more efficient and environmentally friendly and responsible way. Computers consume a lot of natural resources, from the raw materials needed to manufacture them, the power used to run them, and the problems of disposing them at the end of their life cycle. This can include "designing, manufacturing, using, and disposing of computers, servers, and associated subsystems - such as monitors, printers, storage devices, and networking and communications systems - efficiently and effectively with minimal or no impact on the environment".

The objective of Green computing is to reduce the use of hazardous materials, maximize energy efficiency during the product's lifetime, and promote the recyclability or biodegradability of defunct products and factory waste. Such practices include the implementation of energy-efficient Central Processing Units (CPUs), servers and peripherals as well as reduced resource consumption and proper disposal of electronic waste (e-waste).

I. Green Computing Best Practices

Government regulation, however well-intentioned, is only part of an overall green computing philosophy. The work habits of computer users and businesses can be modified to minimize adverse impact on the global environment. Some of such steps for Green IT include the following:

1. Develop a sustainable Green Computing plan

- Involve stakeholders to include checklists, recycling policies, recommendations for disposal of used equipment, government guidelines and recommendations for purchasing green computer equipment in organizational policies and plans;
- Encourage the IT community for using the best practices and encourage them to consider green computing practices and guidelines.
- On-going communication about and campus commitment to green IT best practices to produce notable results.
- Include power usage, reduction of paper consumption, as well as recommendations for new equipment and recycling old machines in organizational policies and plans; and

- Use cloud computing so that multiple organizations share the same computing resources thus increasing the utilization by making more efficient use of hardware resources.

2. **Recycle**

   - Dispose e-waste according to central, state and local regulations;
   - Discard used or unwanted electronic equipment in a convenient and environmentally responsible manner as computers emit harmful emissions;
   - Manufacturers must offer safe end-of-life management and recycling options when products become unusable; and
   - Recycle computers through manufacturer's recycling services.

3. **Make environmentally sound purchase decisions**

   - Purchase of desktop computers, notebooks and monitors based on environmental attributes;
   - Provide a clear, consistent set of performance criteria for the design of products;
   - Recognize manufacturer efforts to reduce the environmental impact of products by reducing or eliminating environmentally sensitive materials, designing for longevity and reducing packaging materials; and
   - Use Server and storage virtualization that can help to improve resource utilization, reduce energy costs and simplify maintenance.

4. **Reduce Paper Consumption**

   - Reduce paper consumption by use of e-mail and electronic archiving;
   - Use of "track changes" feature in electronic documents, rather than red line corrections on paper;
   - Use online marketing rather than paper based marketing; e-mail marketing solutions that are greener, more affordable, flexible and interactive than direct mail; free and low-cost online invoicing solutions that help cut down on paper waste; and

- While printing documents; make sure to use both sides of the paper, recycle regularly, use smaller fonts and margins, and selectively print required pages.

5. **Conserve Energy**

- Use Liquid Crystal Display (LCD) monitors rather than Cathode Ray Tube (CRT) monitors;
- Develop a thin-client strategy wherein thin clients are smaller, cheaper, simpler for manufacturers to build than traditional PCs or notebooks and most importantly use about half the power of a traditional desktop PC;
- Use notebook computers rather than desktop computers whenever possible;
- Use the power-management features to turn off hard drives and displays after several minutes of inactivity;
- Power-down the CPU and all peripherals during extended periods of inactivity;
- Try to do computer-related tasks during contiguous, intensive blocks of time, leaving hardware off at other times;
- Power-up and power-down energy-intensive peripherals such as laser printers according to need;
- Employ alternative energy sources for computing workstations, servers, networks and data centers; and
- Adapt more of Web conferencing offers instead of travelling to meetings in order to go green and save energy.

II. Green IT Security Services and Challenges

IT solution providers are offering green security services in many ways. What to look in green security products, the challenges in the security services market and how security services fare in a recession. If administered properly with other green computing technologies, green security can be a cost-efficient and lucrative green IT service for solution providers. The basic aim is to increase the customer's energy savings through green security services and assess that 'how sustainable computing technology can immediately help the environment'. Green IT services present many benefits for clients as well as providers, but knowing 'how to evaluate a client's infrastructure to accommodate green technology is really a vital issue'.

Moreover, apart from the common security issues, the green security emphasizes the role of security tools, methods and practices that reduce a company's environmental impact. But to estimate the scope, to cope with the lack of green security services in the market and get advice on conserving power and purchasing switches is very important and needs a high level of sensitivity. Learning about the challenges of implementing green security and the best practices is a major hope, as the artifacts are still evolving.

4.8.6 Bring Your Own Device (BYOD)

BYOD (Bring Your Own Device) refers to business policy that allows employees to use their preferred computing devices, like smart phones and laptops for business purposes. It means employees are welcome to use personal devices (laptops, smart phones, tablets etc.) to connect to the corporate network to access information and application. The BYOD policy has rendered the workspaces flexible, empowering employees to be mobile and giving them the right to work beyond their required hours. The continuous influx of readily improving technological devices has led to the mass adoption of smart phones, tablets and laptops, challenging the long-standing policy of working on company-owned devices. Though it has led to an increase in employees' satisfaction but also reduced IT desktop costs for organizations as employees are willing to buy, maintain and update devices in return for a one-time investment cost to be paid by the organization.

In the early 1990s, executing different tasks necessitated the use of different devices. For instance, an mp3 player was needed to listen to music; whereas chores, tasks and schedules were tracked by a PDA. An addition to this, list was a bulky laptop and a camera and it seemed waiting till eternity that we would ever have a single device to suit our different needs. However, remarkable advances in technology in the last decade have made it possible to perform all the above-mentioned tasks using a single hi-tech device. Different technologies can work in synergy with each other, which improves user productivity and convenience.

I. Advantages of BYOD

- **Happy Employees:** Employees love to use their own devices when at work. This also reduces the number of devices an employee has to carry; otherwise he would be carrying his personal as well as organization provided devices.

♦ **Lower IT budgets:** Could involve financial savings to the organization since employees would be using the devices they already possess thus reducing the outlay of the organization in providing devices to employees.

♦ **IT reduces support requirement:** IT department does not have to provide end user support and maintenance for all these devices resulting in cost savings.

♦ **Early adoption of new Technologies:** Employees are generally proactive in adoption of new technologies that result in enhanced productivity of employees leading to overall growth of business.

♦ **Increased employee efficiency:** The efficiency of employees is more when the employee works on his/her own device. In an organization provided devices, employees have to learn and there is a learning curve involved in it.

II. Emerging BYOD Threats

Every business decision is accompanied with a set of threats and so is BYOD program too; it is not immune from them. As outlined in the Gartner survey, a BYOD program that allows access to corporate network, emails, client data etc. is one of the top security concerns for enterprises. Overall, these risks can be classified into four areas as outlined below:

♦ **Network Risks:** It is normally exemplified and hidden in 'Lack of Device Visibility'. When company-owned devices are used by all employees within an organization, the organization's IT practice has complete visibility of the devices connected to the network. This helps to analyze traffic and data exchanged over the Internet. As BYOD permits employees to carry their own devices (smart phones, laptops for business use), the IT practice team is unaware about the number of devices being connected to the network. As network visibility is of high importance, this lack of visibility can be hazardous. For example, if a virus hits the network and all the devices connected to the network need be scanned, it is probable that some of the devices would miss out on this routine scan operation. In addition to this, the network security lines become blurred when BYOD is implemented.

♦ **Device Risks:** It is normally exemplified and hidden in 'Loss of Devices'. A lost or stolen device can result in an enormous financial and reputational embarrassment to an organization as the device may hold sensitive corporate information. Data lost from stolen or lost devices ranks as the top security threats as per the rankings released by Cloud Security Alliance. With easy access to company emails as well as corporate intranet, company trade secrets can be easily retrieved from a misplaced device.

- **Application Risks:** It is normally exemplified and hidden in 'Application Viruses and Malware'. A related report revealed that a majority of employees' phones and smart devices that were connected to the corporate network weren't protected by security software. With an increase in mobile usage, mobile vulnerabilities have increased concurrently. Organizations are not clear in deciding that 'who is responsible for device security – the organization or the user'.
- **Implementation Risks:** It is normally exemplified and hidden in 'Weak BYOD Policy'. The effective implementation of the BYOD program should not only cover the technical issues mentioned above but also mandate the development of a robust implementation policy. Because corporate knowledge and data are key assets of an organization, the absence of a strong BYOD policy would fail to communicate employee expectations, thereby increasing the chances of device misuse. In addition to this, a weak policy fails to educate the user, thereby increasing vulnerability to the above-mentioned threats.

4.8.7 Web 3.0

The term **Web 3.0,** also known as the **Semantic Web**, describes sites wherein the computers will be generated raw data on their own without direct user interaction. Web 3.0 is considered as the next logical step in the evolution of the Internet and Web technologies. Initially, the Internet is confined within the physical walls of the computer, but as more and more devices such as smartphones, cars and other household appliances become connected to the web, the Internet will be omnipresent and could be utilized in the most efficient manner.

I. Underlying Concept

Web 3.0 standard uses semantic web technology, drag and drop mash-ups, widgets, user behavior, user engagement, and consolidation of dynamic web contents depending on the interest of the individual users. Web 3.0 technology uses the "Data Web" Technology, which features the data records that are publishable and reusable on the web through query-able formats.

The Web 3.0 standard also incorporates the latest researches in the field of artificial intelligence.

An example of typical Web 3.0 application is the one that uses content management systems along with artificial intelligence. These systems can answer the questions posed by the users, because the application can think on its own and find the most probable answer, depending on the context, to the query submitted by the user. In this way, Web 3.0 can also be described as a "machine to user" standard in the internet.

II. Components of Web 3.0

- **Semantic Web:** This provides the web user a common framework that could be used to share and reuse the data across various applications, enterprises, and community boundaries. This allows the data and information to be readily intercepted by machines, so that the machines are able to take contextual decisions on their own by finding, combining and acting upon relevant information on the web.
- **Web Services:** It is a software system that supports computer-to-computer interaction over the Internet. For example - the popular photo-sharing website Flickr provides a web service that could be utilized and the developers to programmatically interface with Flickr in order to search for images.

To conclude, Web 3.0 helps to achieve a more connected open and intelligent web applications using the concepts of natural language processing machine learning, machine reasoning and autonomous agents.

As technology evolves new application are coming into use. These applications are further changing the way individuals/businesses/ government interact with each other and do business. Moving ahead, a new concept Web 4.0 is set to evolve; proposed to be autonomous, proactive, content-exploring, self-learning, collaborative, and content-generating agents based on fully matured semantic and reasoning technologies as well as Artificial Intelligence. These services will support adaptive content presentation that will use the Web database via an intelligent agent. Examples might be services interacting with sensors and implants, natural-language services or virtual reality services.

4.8.8 Internet of Things (IoT)

I. Definition: The **Internet of Things (IoT)** is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. For example:

(i) Washing machines with Wi-Fi networking capabilities can connect themselves to home Wi-Fi. Once these machines are so connected, they can be controlled through machine manufacturer mobile APP from anywhere in the world.

(ii) India's living legend of cricket appearing in an Advertisement for water purifier informs that, the water purifier is Wi-Fi enabled. When the purifying agents deplete in the machine, it connects to home Wi-Fi and informs the service agents of the company.

All above examples are from products being sold in India.

II. Future: Gartner, the technology researcher has projected that by 2020 the IOT business across the world would increase to USD 1.9 Trillion. In rupee terms at current exchange rate (INR::UDS=67.50::1) it comes to a staggering ₹ 1,34,0,00,00,00,00,000.00 or keeping it simple virtually equal to India's GDP today.

III. Applications: Some of the applications are as follows:

♦ All home appliances to be connected and that shall create a virtual home.

  a. Home owners can keep track of all activities in house through their hand-held devices.

  b. Home security CCTV is also monitored through hand held devices.

♦ Office machines shall be connected through net.

  a. Human resource managers shall be able to see how many people have had a cup of coffee from vending machine and how many are present.

  b. How many printouts are being generated through office printer?

♦ Governments can keep track of resource utilizations / extra support needed.

a. Under SWACHH mission government can tag all dustbins with IOT sensors. They (dustbins) generate a message once they are full. Being connected to Wi-Fi, they can intimate the cleaning supervisor of Municipal Corporation so that BIN can be emptied.

- As a research study, individuals have got themselves implanted with electronic chips in their bodies. This chip allows him / her to connect to home / office Wi-Fi. Once connected person can enter home / office and perform designated function. This chip becomes individual's authentication token.
- ***Wearables:*** ***Just like smart homes, wearables remain another important potential IoT application like Apple smartwatch.***
- ***Smart City:*** ***Smart cities, like its name suggests, is a big innovation and spans a wide variety of use cases, from water distribution and traffic management to waste management and environmental monitoring.***
- ***Smart Grids:*** ***Smart grids are another area of IoT technology that stands out. A smart grid basically promises to extract information on the behaviors of consumers and electricity suppliers in an automated fashion to improve the efficiency, economics, and reliability of electricity distribution.***
- ***Industrial Internet of things:*** ***One way to think of the Industrial Internet is by looking at connected machines and devices in industries such as power generation, oil, gas, etc. for monitoring and improving control efficiency. With an IoT enabled system, factory equipment that contains embedded sensors communicate data about different parameters, such as pressure, temperature, and utilization of the machine. The IoT system can also process workflow and change equipment settings to optimize performance.***
- ***Connected Car:*** ***Connected car technology is a vast and an extensive network of multiple sensors, antennas, embedded software, and technologies that assist in communication to navigate in our complex world.***
- ***Connected Health (Digital Health/Telehealth/Telemedicine):*** ***IoT has various applications in healthcare, which are from remote monitoring equipment to advance and smart sensors to equipment***

integration. It has the potential to improve how physicians deliver care and keep patients safe and healthy.

- ***<u>Smart Retail:</u> Retailers have started adopting IoT solutions and using IoT embedded systems across several applications that improve store operations, increasing purchases, reducing theft, enabling inventory management, and enhancing the consumer's shopping experience.***
- ***<u>Smart Supply Chain:</u> Supply chains have already been getting smarter for a couple of years. Offering solutions to problems like tracking of goods while they are on the road or in transit or helping suppliers exchange inventory information are some of the popular offerings.***

IV. **Risks:** Internet of thing is an evolving phenomenon. The nature of risk is carries is based on academic logics and available practical experiences. The risk listed are those which are most discussed for IOT today. As technology evolves issues shall crop up. The risk due to IOT has various facets to it:

(A) Risk to Product manufacturer

Manufacturers may be out of business in few years if IoT becomes a necessary product feature.

- **Data storage and analytics:** The manufacturers will to ensure the huge data generated from IOT devices is kept secured. Hacking / Loosing this data may be distractors for entity as well as the individual to whom it relates to.

(B) Risk to user of these products

- **Security:** This is the greatest risk due to IOT. As home devices / office equipment's are connected to network they shall be hit by all network related risks, including hacking, virus attacks, stealing confidential data etc.
- **Privacy, autonomy and control:** There is a huge risk that individuals may lose control over their personal life. Their personal life can be hacked and made public. The other major concern is who has the ownership of this personal data. For example: A person daily eats a burger at 12.00 in night and takes bottle of chilled hard drink with it. S/he uses his / her mobile to operate the griller and refrigerator. The griller and refrigerator are both sold by say XYZ ltd. This data is available on XYZ database.

- o Who owns this information?
- o The data can be used by insurance companies to deny an insurance claim saying the person was a habitual drinker or raise his / her medical insurance premium as the person is having a risky life style.

  Above illustrates the big risk IOT may create for individuals.

- ♦ **Intentional obsolescence of devices:** This may happen due to -
  - o Companies which want to bring a new product may force users to dump the old products. This they can do by disabling the operating software of old product.
  - o A manufacturer is bought out by another manufacturer. The buyer does not support old products sold.

(C) Technology Risk

Platform fragmentation and lack of technical standards are situations where the variety of IoT devices, in terms of both hardware variations and differences in the software running on them, makes the task of developing applications tough.

(D) Environmental Risk due to Technology

These studies are being done to see the impact on house air quality, due to use of heavy earth metals in devices. There no definitive data available as of now, but the risk is being considered.

4.8.9 Artificial Intelligence (AI)

I. Definition: Intelligence, as defined in Chambers dictionary; "The ability to use memory, knowledge, experience, understanding, reasoning, imagination and judgement to solve problems and adapt to new situations". The ability described above when exhibited by machines is called as **Artificial intelligence (AI)**. It is intelligence exhibited by machines. For example:

i. This technology is being used in autonomous vehicles, the google car.

ii. Apple online assistant Siri is supposed to use it.

II. Applications

Artificial Intelligence is being used in the following applications:

- ♦ Autonomous vehicles (such as drones and self-driving cars);

- ♦ Medical diagnosis, in cancer research. Predicting the chances of an individual getting ill by a disease;
- ♦ Creating art (such as poetry);
- ♦ Proving mathematical theorems;
- ♦ Playing games (such as Chess or Go), and predicting the outcomes. Say which number on a lottery ticket may win;
- ♦ Search engines (such as Google search);
- ♦ Online assistants (such as Siri);

III. Risks

1. AI relies heavily of data it gets. Incorrect data can lead to incorrect conclusions.
2. AI (robots) carries a security threats. Countries are discussing to have a KILL button in all AI capable machines. This is important otherwise someday machine may start controlling humans.
3. AI in long term may kill human skills of thinking the unthinkable. All data shall be processed in a structured manner, where machines shall provide solution based on their learning over a period of time. These machines shall not have capability of thinking out of box.

IV. Controls

The set of controls in AI will be extremely complex because of the nature of processing of information and must be dealt with based on the nature of the AI tool and the purpose, etc.

4.8.10 Machine Learning

I. Definition: Machine Learning is a type of Artificial Intelligence (AI) that provides computers with the ability to learn without being explicitly programmed. Machine learning focuses on the development of computer programs that can change when exposed to new data. The process of machine learning is similar to that of data mining. For example:

- ♦ Machine learning has been used for image, video, and text recognition, as well as serving as the power behind recommendation engines. Apple SIRI is a good example.
- ♦ This technology is being is being used in autonomous vehicles, the google car.

II. **Applications:** Virtually all applications were in AI using Machine learning so that some value is added. It includes specifically following application:

1. Autonomous vehicles (such as drones and self-driving cars),
2. Medical diagnosis, in cancer research. Predicting the chances of an individual getting ill by a disease.
3. Playing games (such as Chess or Go), and predicting the outcomes. Say which number on a lottery ticket may win.
4. Search engines (such as Google search),
5. Online assistants (such as Siri),

III. **Risk:** Machine learning being an application based on AI, the nature of risk to it remain similar to those posed by AI systems.

4.9 CASE STUDIES

I. **Category: Flipkart started as e-commerce and has now moved to m-commerce space.**

Back in 2007, when Flipkart was launched, Indian **e-commerce** industry was taking its beginner steps. The company is registered in Singapore, but their headquarters are in the city of Bangalore, India. The promoters are Binny Bansal and Sachin Bansal. They left their jobs in Amazon to start their own business. One can easily call that a risky move.

Flipkart began selling books to begin with. It soon expanded and began offering a wide variety of goods. Innovating right from the start, Flipkart has been home to few of the striking features of Indian e-commerce. Flipkart success in the first few years of its existence. Flipkart raised funds through venture capital funding. As the company grew in stature, more funding arrived.

Flipkart addressed to major issues in online purchasing in India. Indians love to pay after checking the products so Flipkart was the first to implement the popular **'Cash On Delivery'** facility, which every online shopping website in India offers as an option today. Second major issue Flipkart addressed was timely delivery. It was more of a cultural revolution to ensure the whole supply chain was revamped and sensitized to issue of timely delivery.

II. **Category: JUGNOO started as a m-commerce company.**

Jugnoo is an auto-rickshaw aggregator, focused on doubling the driver's efficiency and earnings, and providing affordable transportation to the masses on a tap. There are around 5 million auto-rickshaws in our country, whereas the utilization is only 30%. It started operation in October 2014 from Chandigarh.

Despite being one of the most popular and economical modes of public transportation in India, auto-rickshaws have remained highly underutilized due to inefficiencies prevalent in the conventional hailing procedure such as availability and fares. Jugnoo was started with a vision to overcome these roadblocks by bringing structure into this space, aggregating auto-rickshaws via technology, thereby, enabling optimum utilization of resources.

III. Category: OYO started as a m-commerce company.

OYO means **"ON YOUR OWN"**. OYO Rooms was nothing but an idea to create India's largest chain of efficient, young, standardized rooms with an intention to build the coolest chain of no add-on rooms which might not have Spa, Gym etc. like the star hotels but will live upto the basic standards & high expectations for prices like never before. They have few basic amenities including, clean rooms, clean linen, AC, clean bathroom, free Wi-Fi, free breakfast.

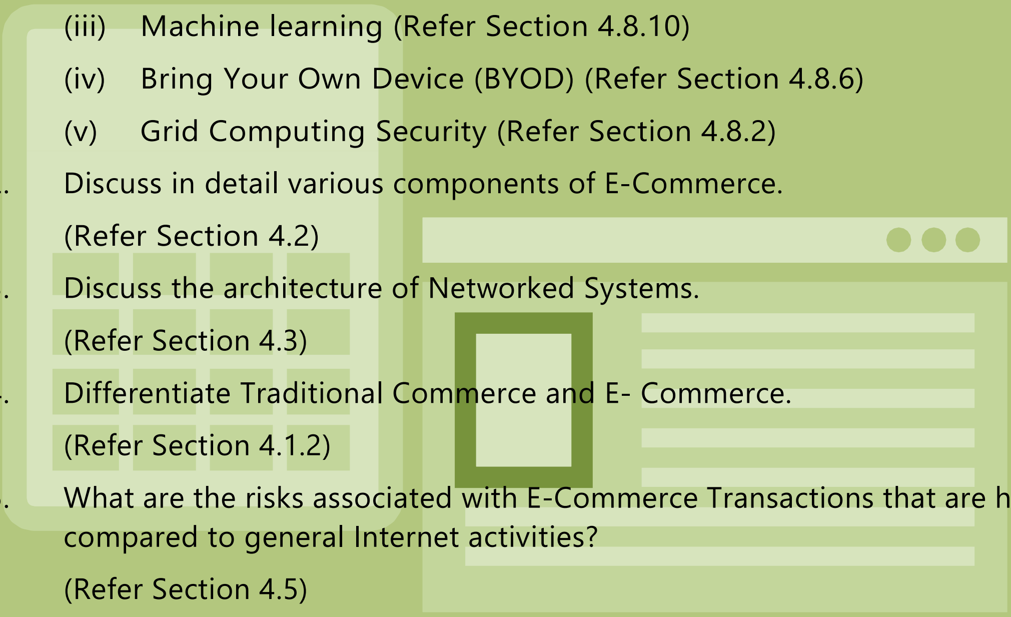
The teenage boy – Ritesh Agarwal is the young Founder and CEO of OYO Rooms - fastest growing Branded network of hotels offline & online. OYO rooms do nothing out of the box but provides travelers the coolest yet cheapest efficient, young, standardized rooms with no add-ons attached to it!

SUMMARY

Today electronic commerce is ruling the world. Every day there is a start-up in the e-commerce / m-commerce space. This is forcing traditional businesses to adopt to this new way of doing business. E-commerce/M-commerce both have related sets of risks and necessary controls to be put in place. They are generating huge benefits to society in terms of saving costs and time. E-commerce and M-commerce being the new way doing business has its run ins with law also. The legality/implications of such transactions are being tested in courts across the world including India. Laws are being updated / amended to keep pace with these new business trends. Emerging technology like Internet of Things, AI, Machine learning is changing the way humans interact with technology. These technologies are automating human tasks and creating options to carry those tasks which could not have done previously.

TEST YOUR KNOWLEDGE

Theory Questions



1. Define the following:
   - (i) E- Commerce (Refer Section 4.1)
   - (ii) M-Commerce (Refer Section 4.3.4)
   - (iii) Machine learning (Refer Section 4.8.10)
   - (iv) Bring Your Own Device (BYOD) (Refer Section 4.8.6)
   - (v) Grid Computing Security (Refer Section 4.8.2)
2. Discuss in detail various components of E-Commerce.

   (Refer Section 4.2)
3. Discuss the architecture of Networked Systems.

   (Refer Section 4.3)
4. Differentiate Traditional Commerce and E- Commerce.

   (Refer Section 4.1.2)
5. What are the risks associated with E-Commerce Transactions that are high as compared to general Internet activities?

   (Refer Section 4.5)
6. Explain efficiency improvement due to E- Business.

   (Refer Section 4.1.4)
7. Define the Guidelines for E - Commerce.

   (Refer Section 4.6.1)
8. Explain the types of Network Architecture.

   (Refer Section 4.3)
9. What are the ways of protecting your e-Commerce business from intrusion?

   (Refer Section 4.5)
10. Explain Digital Payments? Define different Types of Digital Payments?

    (Refer Section 4.7)
11. What are some drawbacks of Digital Payments?

    (Refer Section 4.7.3)

12. What do you mean by "Cloud Computing"? Discuss its characteristics.
    (Refer Section 4.8.3)

13. Differentiate between different types of clouds in Cloud Computing.
    (Refer Section 4.8.3)

14. Discuss various components of Mobile Computing.
    (Refer Section 4.8.3)

15. Discuss some best practices of Green Computing.
    (Refer Section 4.8.3)

Multiple Choice Questions

1. Which one of the following is not an Operating system?
   (a) Android
   (b) Blackberry OS
   (c) FireFox OS
   (d) Chrome OS

2. In two-tier architecture, ____________ is an interface that allows user to interact with the e-commerce / m-commerce vendor.
   (a) Presentation Tier
   (b) Database Tier
   (c) Physical Tier
   (d) Application Tier

3. FEMA stands for ___________.
   (a) Foreign Exchange Management Activity
   (b) Foreign Exchange Management Act
   (c) Foreign Exchange Managerial Act
   (d) Foreign Enterprise Management Act

4. UPI stands for _________.
   (a) Universal Payment Interface
   (b) Unified Proximity Interface
   (c) Unified Payment Interface
   (d) Unified Payment Interaction

5. BHIM (Bharat Interface for Money) is an example of __________.

   (a) Mobile App

   (b) Mobile Hardware

   (c) Mobile Operating System

   (d) Mobile Wallet

6. Which of the following is not a best practice under Green Computing?

   (a) Dispose e-waste according to central, state and local regulations

   (b) Purchase of desktop computers, notebooks and monitors based on environmental attributes

   (c) Power-down the CPU and all peripherals during extended periods of inactivity

   (d) Use Cathode Ray Tube (CRT) monitors than Liquid Crystal Display (LCD) monitors

7. GSM stands for ___________.

   (a) Global Service for Mobile Communication

   (b) Global System for Mobile Communication

   (c) Global Semantics for Mobile Communication

   (d) Global System for Mobile Code

8. Which of the following is the correct sequence of Mobile Computing?

   (i) The user enters or access data using the application on handheld computing device.

   (ii) Now both systems (handheld and site's computer) have the same information and are in sync.

   (iii) The process work the same way starting from the other direction.

   (iv) Using one of several connecting technologies, the new data are transmitted from handheld to site's information system where files are updated and the new data are accessible to other system user.

   (a) (i), (ii), (iii), (iv)

   (b) (iv), (iii), (ii), (i)

   (c) (i), (ii), (iv), (iii)

   (d) (i), (iv), (ii), (iii)

9. AEPS stands for ________________________.

   (a) Aadhaar Enabled Payment Station

   (b) Aadhaar Employed Payment Service

   (c) Aadhaar Enabled Payment Service

   (d) Aadhaar Enterprise Payment Service

10. Which instance of SaaS allows users to explore functionality of Web services such as Google Maps, Payroll processing, and credit card processing services etc.?

   (a) Testing as a Service (TaaS)

   (b) Communication as a Service (CaaS)

   (c) Data as a Service (DaaS)

   (d) API as a Service (APIaaS)

Answers

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

CHAPTER 5

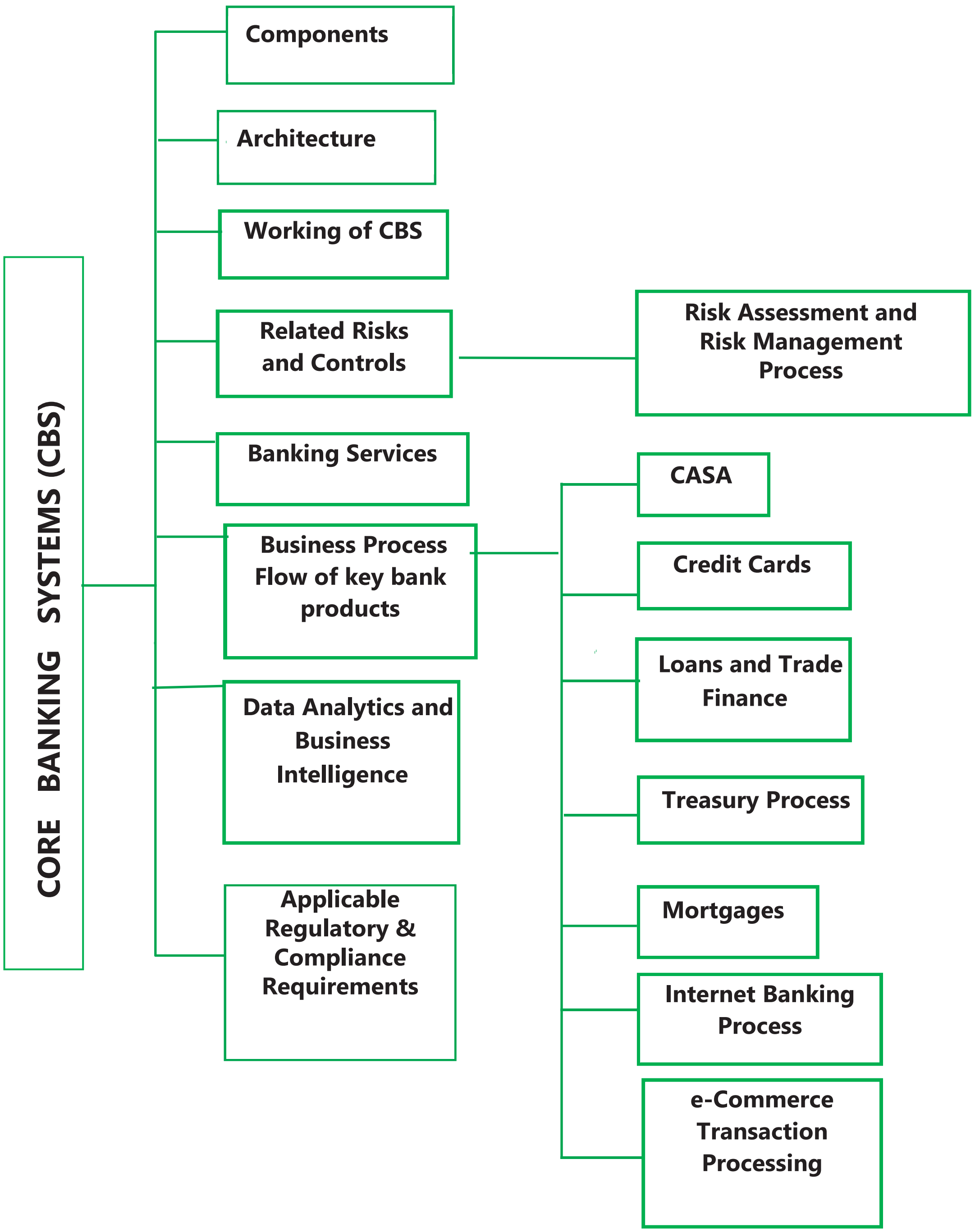
CORE BANKING SYSTEMS

LEARNING OUTCOMES

After reading this chapter, you will be able to -

- □ Understand components and architecture of CBS and impact of related risks and controls.
- □ Appreciate the functioning of core modules of banking and business process flow and impact of related risks and controls.
- □ Comprehend regulatory and compliance requirements applicable to CBS such as Banking Regulations Act, RBI regulations, Prevention of Money Laundering Act and Information Technology Act.

CHAPTER OVERVIEW


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

5.1 OVERVIEW OF BANKING SERVICES

5.1.1 Introduction

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

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

1. Information Technology (IT) is an integral aspect of functioning of enterprises and professionals in this digital age. This has now made banking services increasingly digital with IT plays a very critical role. The rapid strides in IT and the rapid adoption of technology by banks have empowered banks to use it extensively to offer newer products and services to its customers.
2. India as a country could not let behind from global business opportunities. Ushering of reforms by successive governments led to huge growth in India's global business. Customers also sought banks to provide services that enabled them to compete in global economy as well as create new business opportunities in India. As business grew so the need of customer also grew.
3. Successive governments focus to have financial inclusion for all Indians. Banks were found to be most capable of helping government achieve this goal.
4. Growth of internet penetration across India.

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

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

5.1.2 Overview of Banking Services

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

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

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

I. Acceptance of Deposits

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

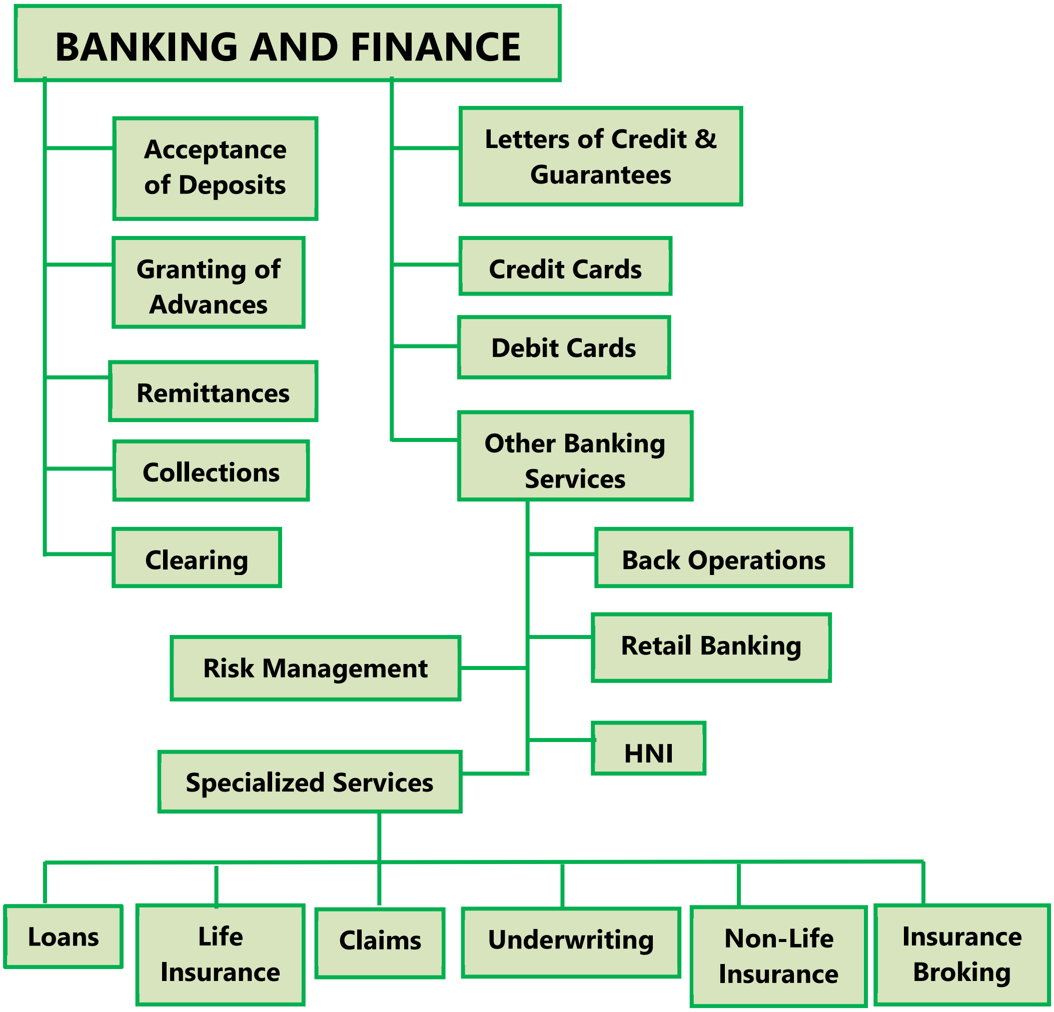


Fig. 5.1.1: Banking and Finance Services

II. Granting of Advances

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

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

III. Remittances

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

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

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

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

IV. Collections

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

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

V. Clearing

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

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

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

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

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

VI. Letters of Credit and Guarantees

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

VII. Credit Cards

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

VIII. Debit Cards

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

IX. Other Banking Services

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

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

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

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

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

5.1.3 Overview of Core Banking Systems (CBS)

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

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

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

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

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

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

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

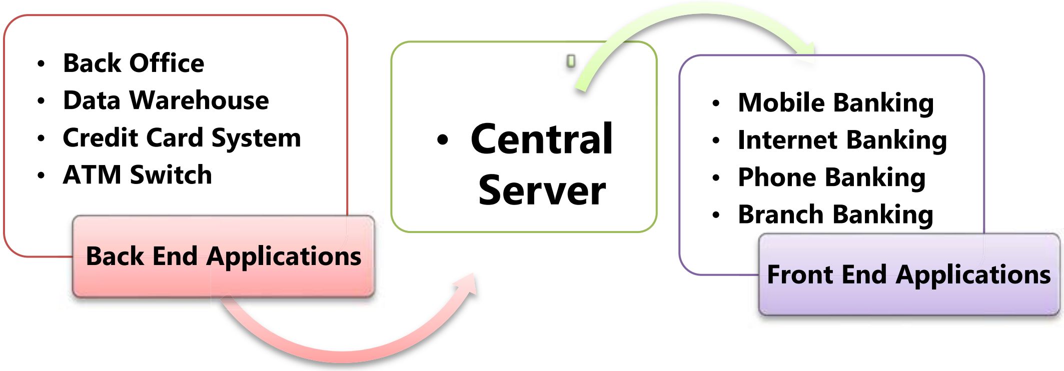


Fig. 5.1.2: Key Modules of CBS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.1.4 Core features of CBS

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

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

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

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

5.2 COMPONENTS AND ARCHITECTURE OF CBS

5.2.1 Technology Components of CBS

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

The key technology components of CBS are as follows:

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

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

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

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

5.2.2 CBS IT Environment

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

These concepts are further explained below.

A. Application Server

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

B. Database Server

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

C. Automated Teller Machines (ATM) Channel Server

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

D. Internet Banking Channel Server (IBCS)

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

E. Internet Banking Application Server

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

F. Web Server

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

G. Proxy Server

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

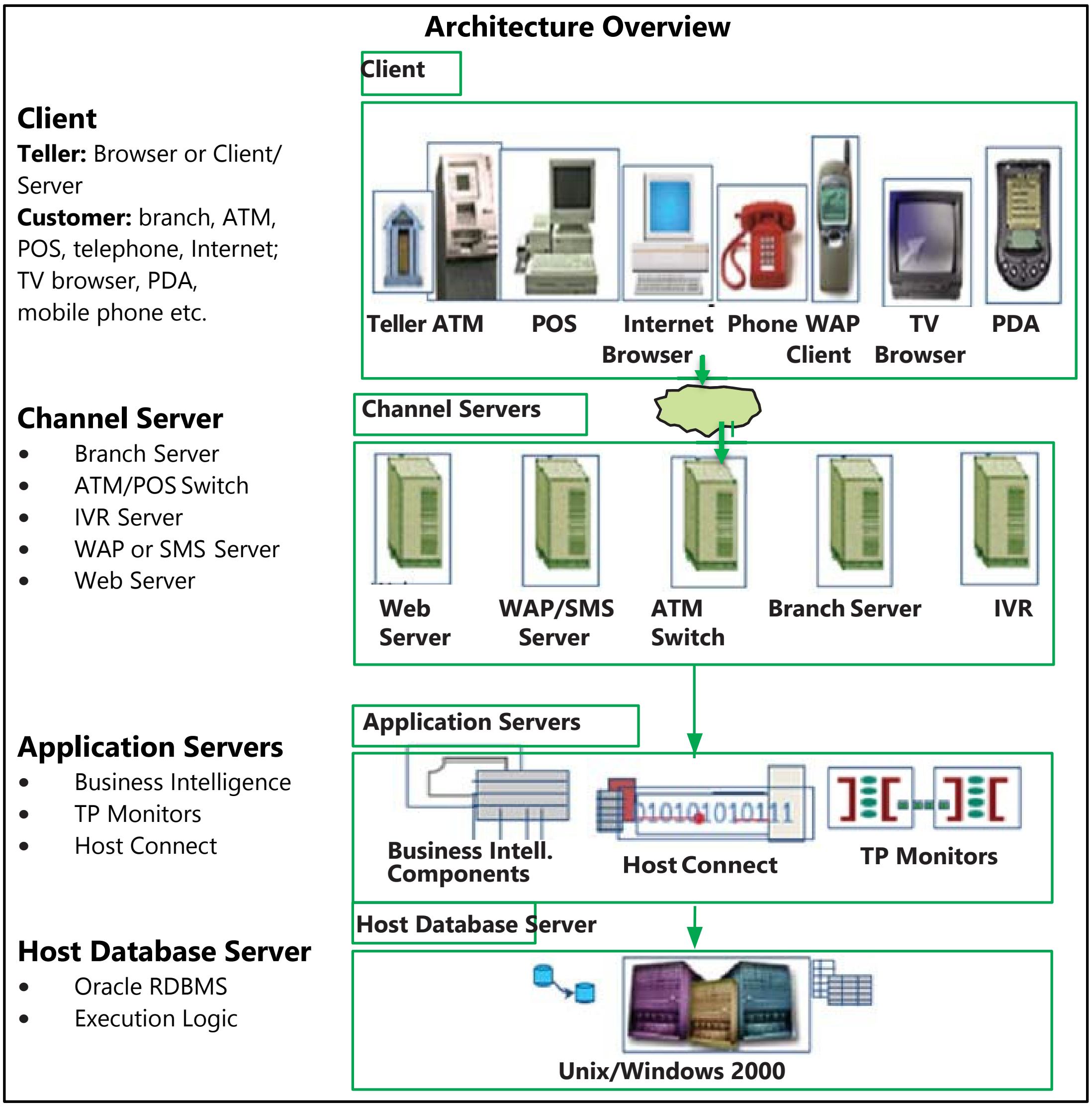


Fig. 5.2.1: CBS IT Environment

H. Anti-Virus Software Server

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

5.2.3 Functional Architecture of CBS

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

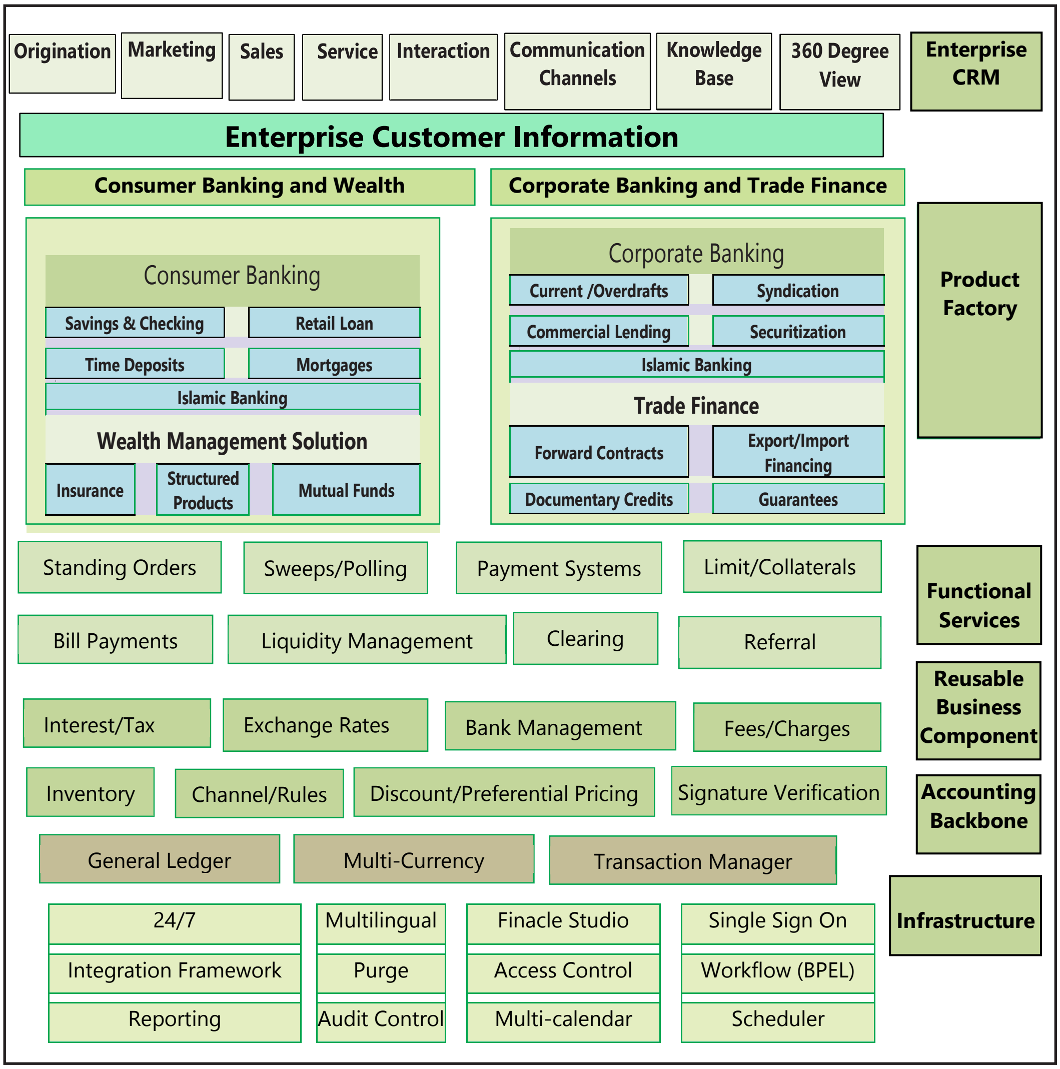


Fig. 5.2.2: Functional Architecture of CBS[1] (Illustrative)

[1] Source: Finacle

5.2.4 Internet Banking Process

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

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

  (a) Password change

  (b) Balance inquiry

  (c) Fund transfer

  (d) Request for cheque book

  (e) Stop payment

  (f) Copy of statement of account; and

  (g) ATM/ Credit Card related queries

- The customer then chooses one of the services from the list. The service requested is directed by the web server to the IBAS for processing. The IBAS will access the internet banking database server for further processing.

- The Internet Banking Channel Server (IBCS) will retrieve the data from the central database server. The IBCS will be able to access the central database server only through a middleware and firewall. The middleware is expected to convert the data to suit the requirements of IBCS.

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

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

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

5.2.5 e-Commerce Transaction processing

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

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

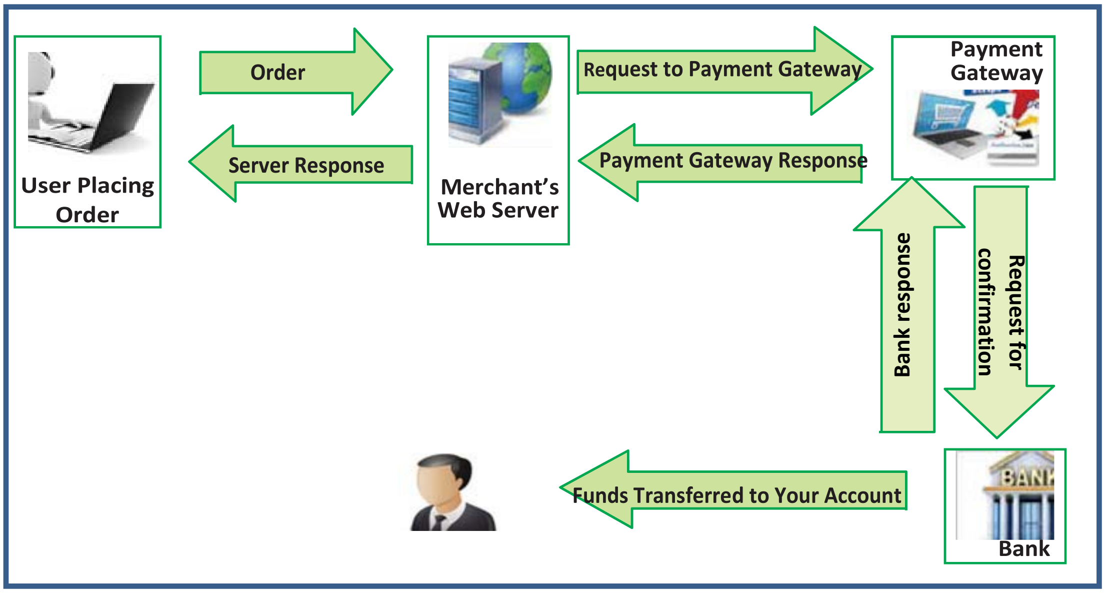


Fig. 5.2.3: e-Commerce Transaction flow for approval of payments

5.2.6 Case Study of IT deployment in Bank

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

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

5.2.7 Implementation of CBS

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

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

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

5.3 CBS RISKS, SECURITY POLICY AND CONTROLS

5.3.1 Risks associated with CBS

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

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

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

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

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

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

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

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

o **Ownership of Data/ process:** Data resides at the Data Centre. Establish clear ownership.

o **Authorization process:** Anybody with access to the CBS, including the customer himself, can enter data directly. What is the authorization process? ***If the process is not robust, it can lead to unauthorized access to the customer information.***

o **Authentication procedures:** ***Usernames and Passwords, Personal Identification Number (PIN), One Time Password (OTP) are some of the most commonly used authentication methods.*** However, these may be inadequate and hence the user entering the transaction may not be determinable or traceable.

o **Several software interfaces across diverse networks:** A Data Centre can have as many as 75-100 different interfaces and application software. ***A data center must also contain adequate infrastructure, such as power distribution and supplemental power subsystems, including electrical switching; uninterruptable power supplies; backup generators and so on. Lapse in any of these may lead to real-time data loss.***

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

5.3.2 Security Policy

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

Information Security

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

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

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

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

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

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

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

5.3.3 Internal Control System in Banks

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

(a) Internal Controls in Banks

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

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

(b) IT Controls in Banks

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

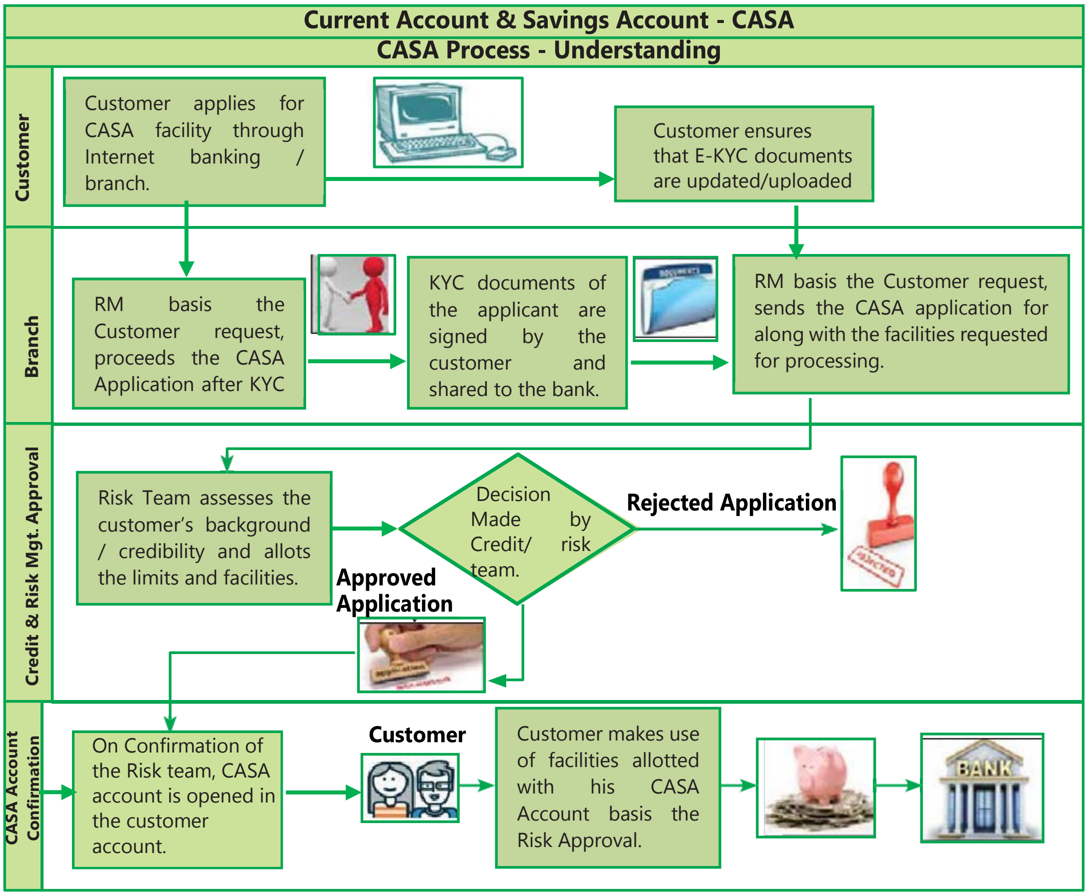

Current Account & Savings Account - CASA
CASA Process - Understanding
Customer
Customer applies for CASA facility through Internet banking / branch.
Customer ensures that E-KYC documents are updated/uploaded
Branch
RM basis the Customer request, proceeds the CASA Application after KYC
KYC documents of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

Fig. 5.3.1: CASA Process

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

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

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

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

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

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

Table 5.3.3: Risk & Controls around the CASA Process

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

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

II. Business Process flow of Credit Cards

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

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

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

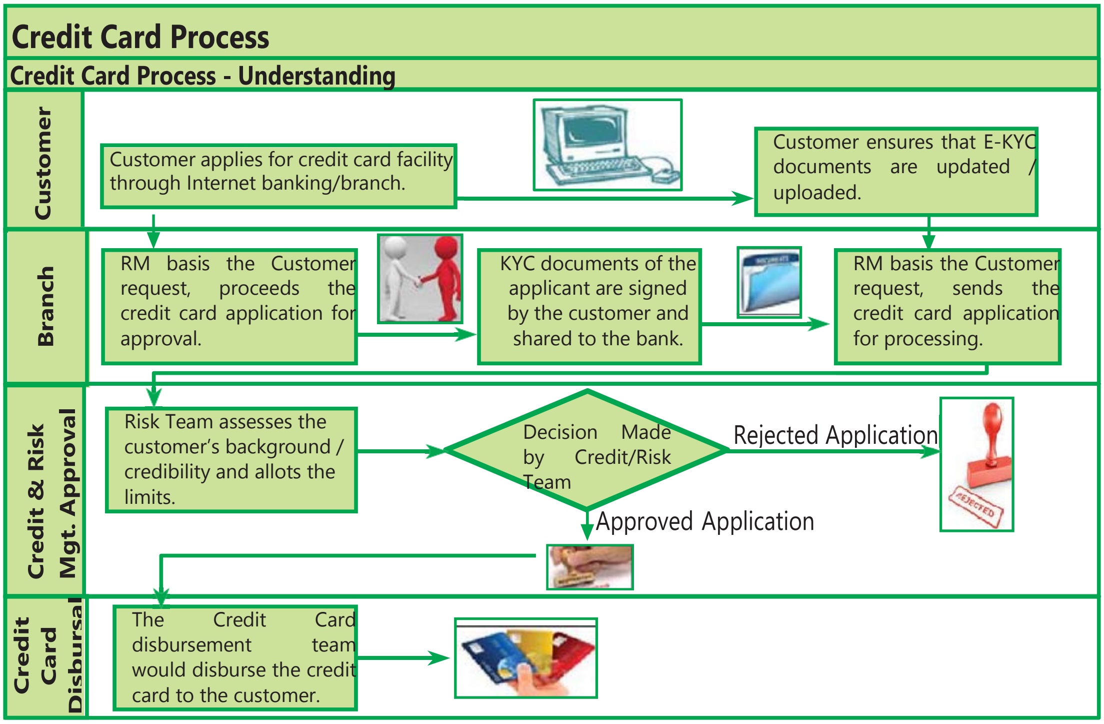

Credit Card Process
Credit Card Process - Understanding
Customer
Branch
Credit & Risk Mgt. Approval
Credit Card Disbursal
Customer applies for credit card facility through Internet banking/branch.
Customer ensures that E-KYC documents are updated / uploaded.
RM basis the Customer request, proceeds the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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

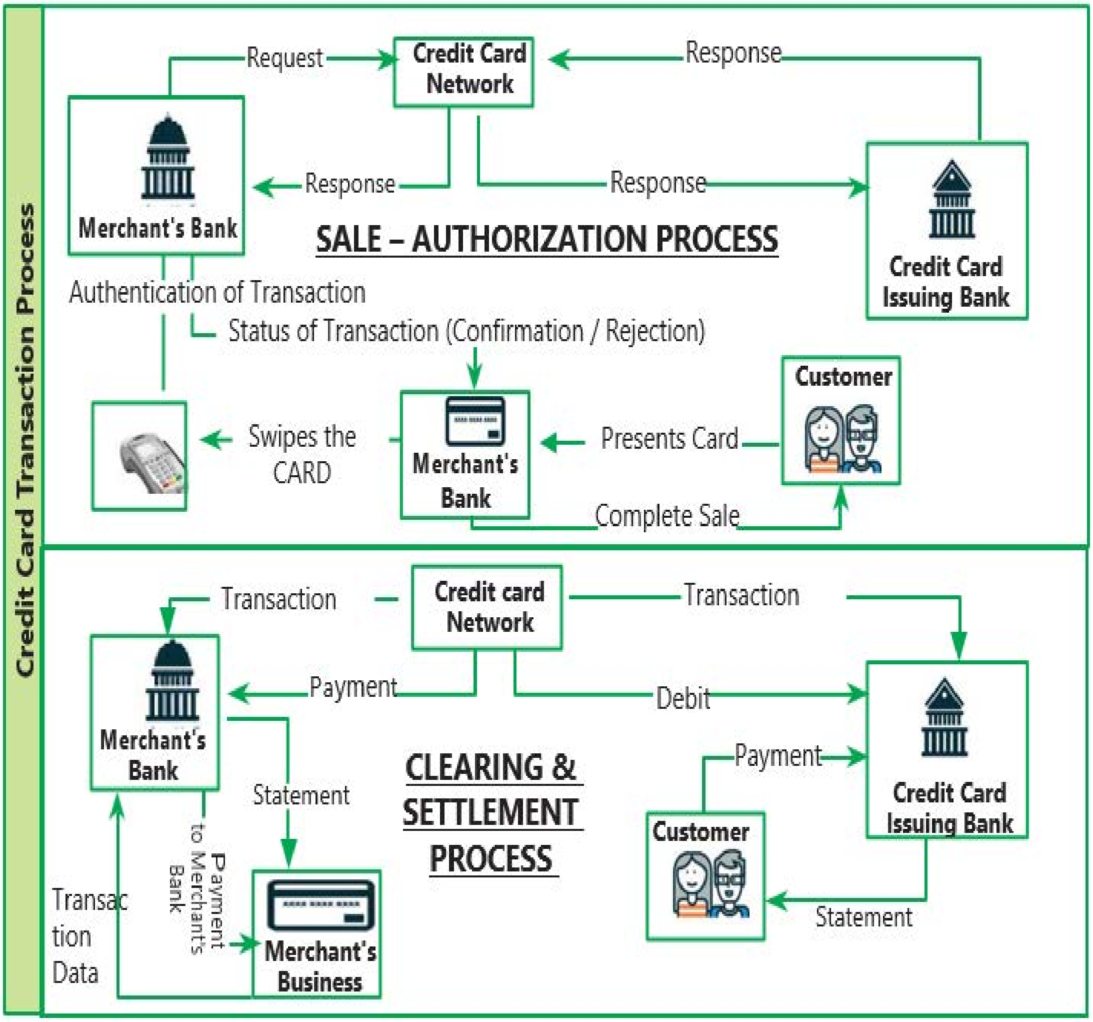


Fig. 5.3.3: Process Flow of Sale - Authorization and Clearing & Settlement of Credit Card Facility

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

Table 5.3.4: Risks and Controls around the Credit Card Process

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

III. Business Process Flow of Mortgages

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

(a) Types of Mortgage Loan

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

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

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

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

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

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

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

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

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

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

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

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

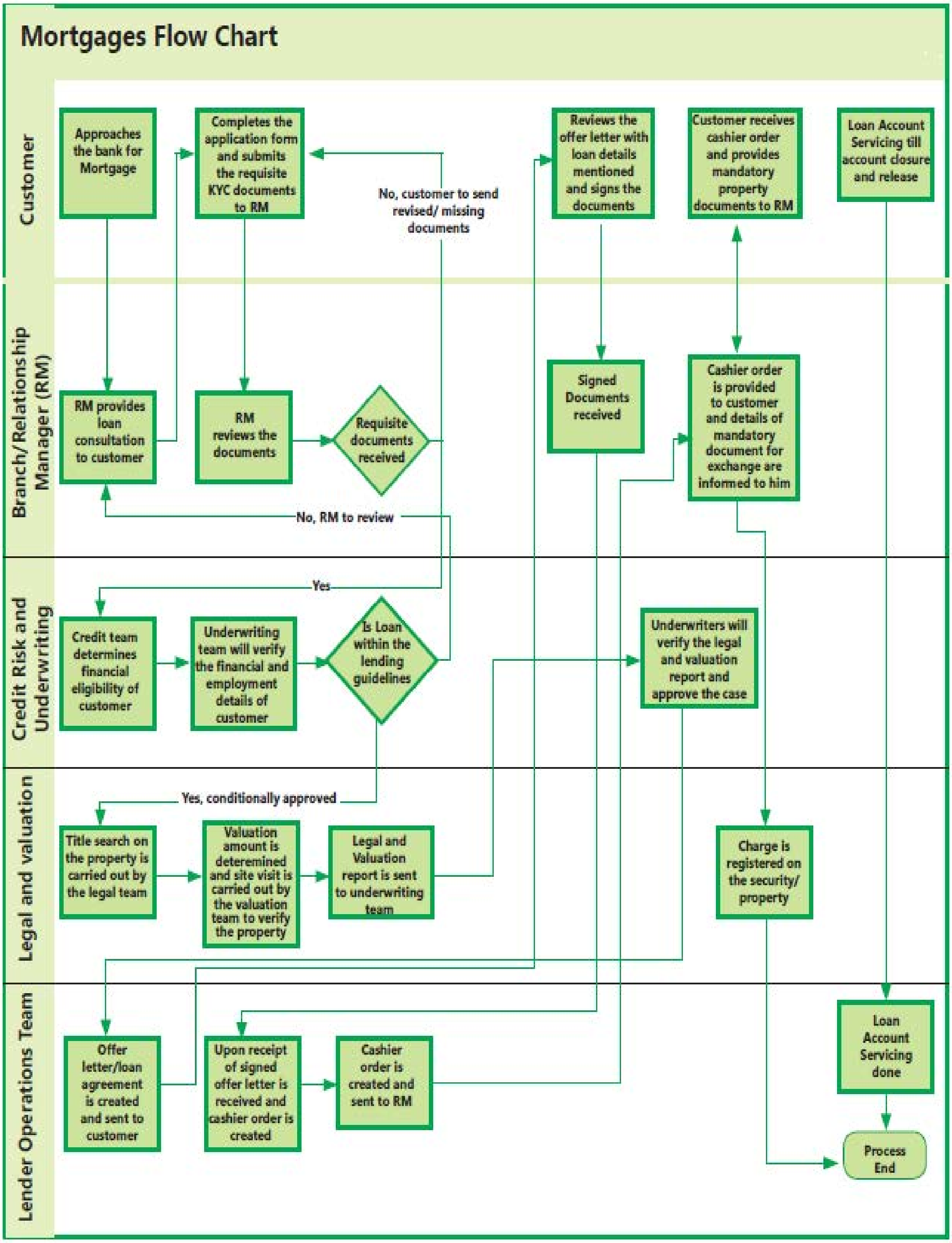

Mortgages Flow Chart
Customer
Branch/Relationship Manager (RM)
Credit Risk and Underwriting
Legal and valuation
Lender Operations Team
Approaches the bank for Mortgage
Completes the application form and submits the requisite KYC documents to RM
No, customer to send revised/ missing documents
Reviews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

Fig. 5.3.4: Business process flow of Mortgages

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

Table 5.3.5: Risk & Controls around the Mortgage Process

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

IV. Business Flow of Treasury Process

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

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

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

- Dealing Room Operations (Front office operations);
- Middle Office (Market Risk department / Product Control Group); and
- 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 modeling associated with derivatives trading and hedging. It is also responsible for monitoring of counter- party, country, dealer and market-related limits that have been set and approved in other areas of the bank such as the credit department.

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

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

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

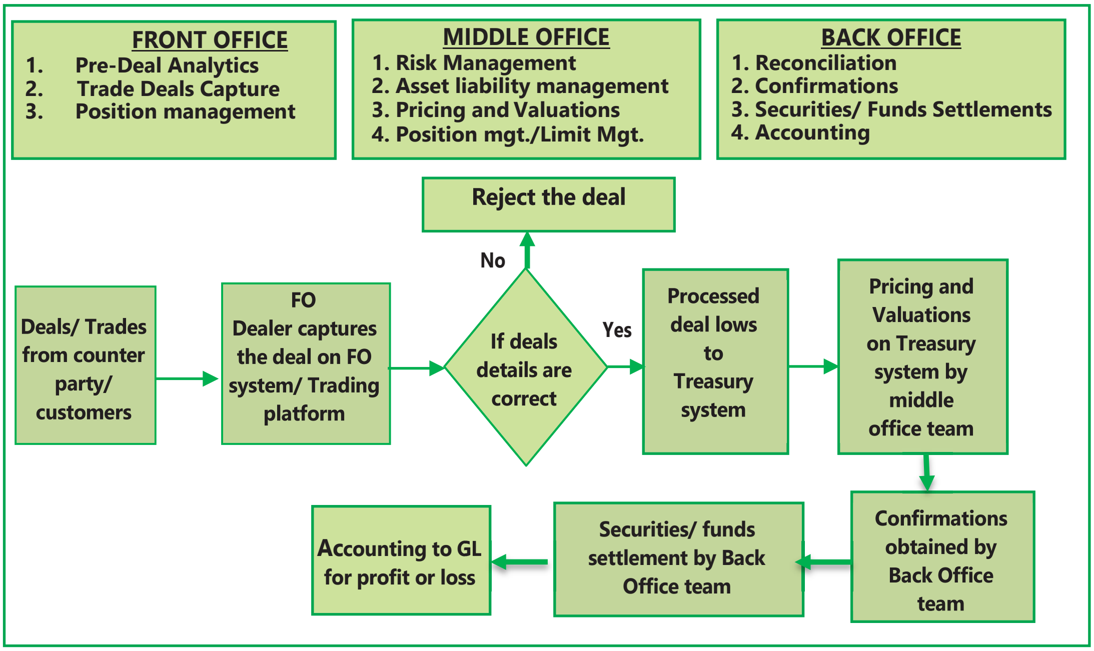

FRONT OFFICE
1. Pre-Deal Analytics
2. Trade Deals Capture
3. Position management
MIDDLE OFFICE
1. Risk Management
2. Asset liability management
3. Pricing and Valuations
4. Position mgt./Limit Mgt.
BACK OFFICE
1. Reconciliation
2. Confirmations
3. Securities/ Funds Settlements
4. Accounting
Reject the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

Fig. 5.3.6: Process Flow for Bank Treasury Operations

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

Table 5.3.6: Risk & Controls around the Treasury Process

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

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

V. Loans and Trade Finance Process

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(II) Loan Disbursal / Facility Utilization and Income Accounting

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

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

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

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

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

Table 5.3.7: Risk & Controls around the Treasury Process

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

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

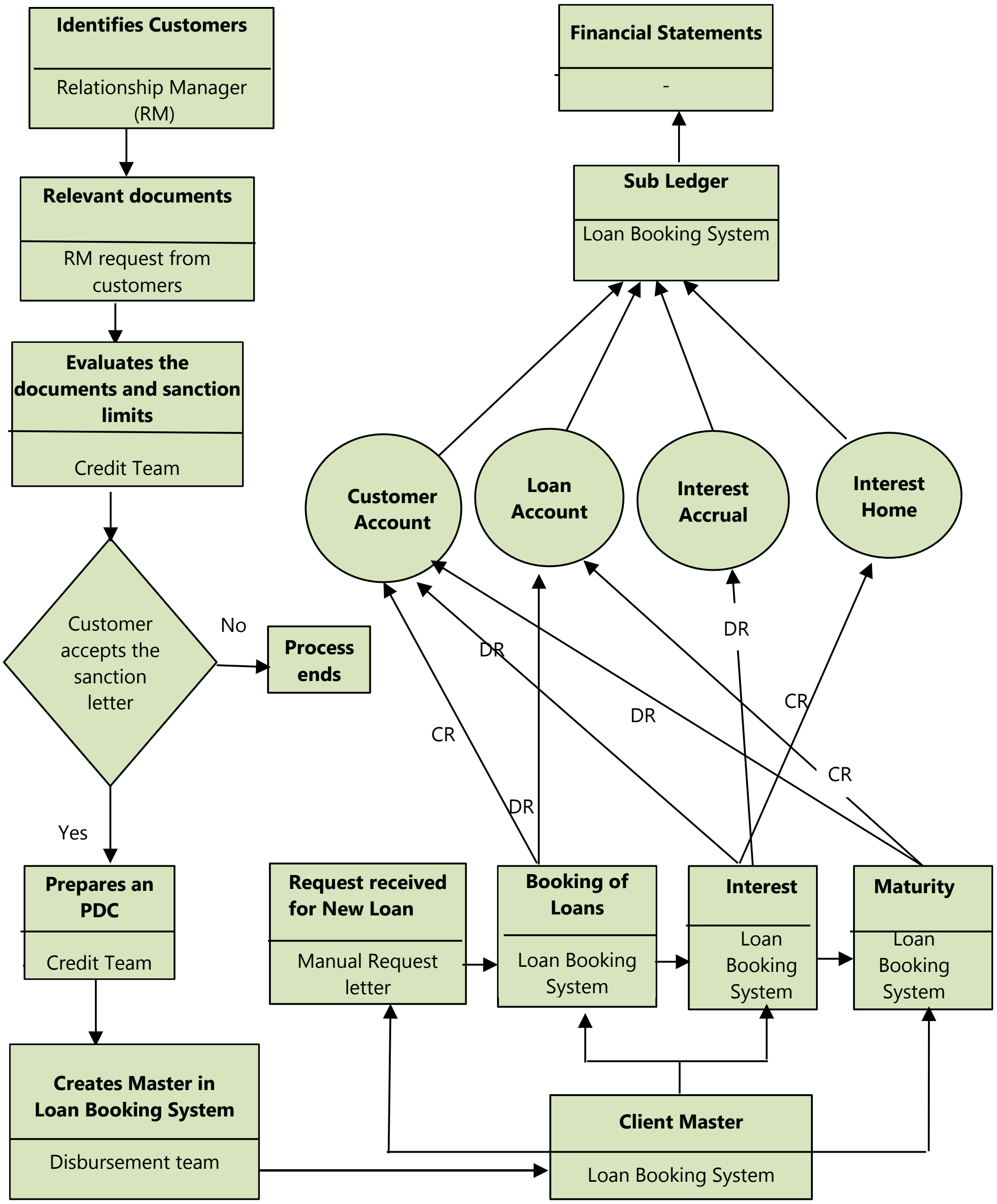


Fig. 5.3.6: Process Flow for Fund based Loans

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

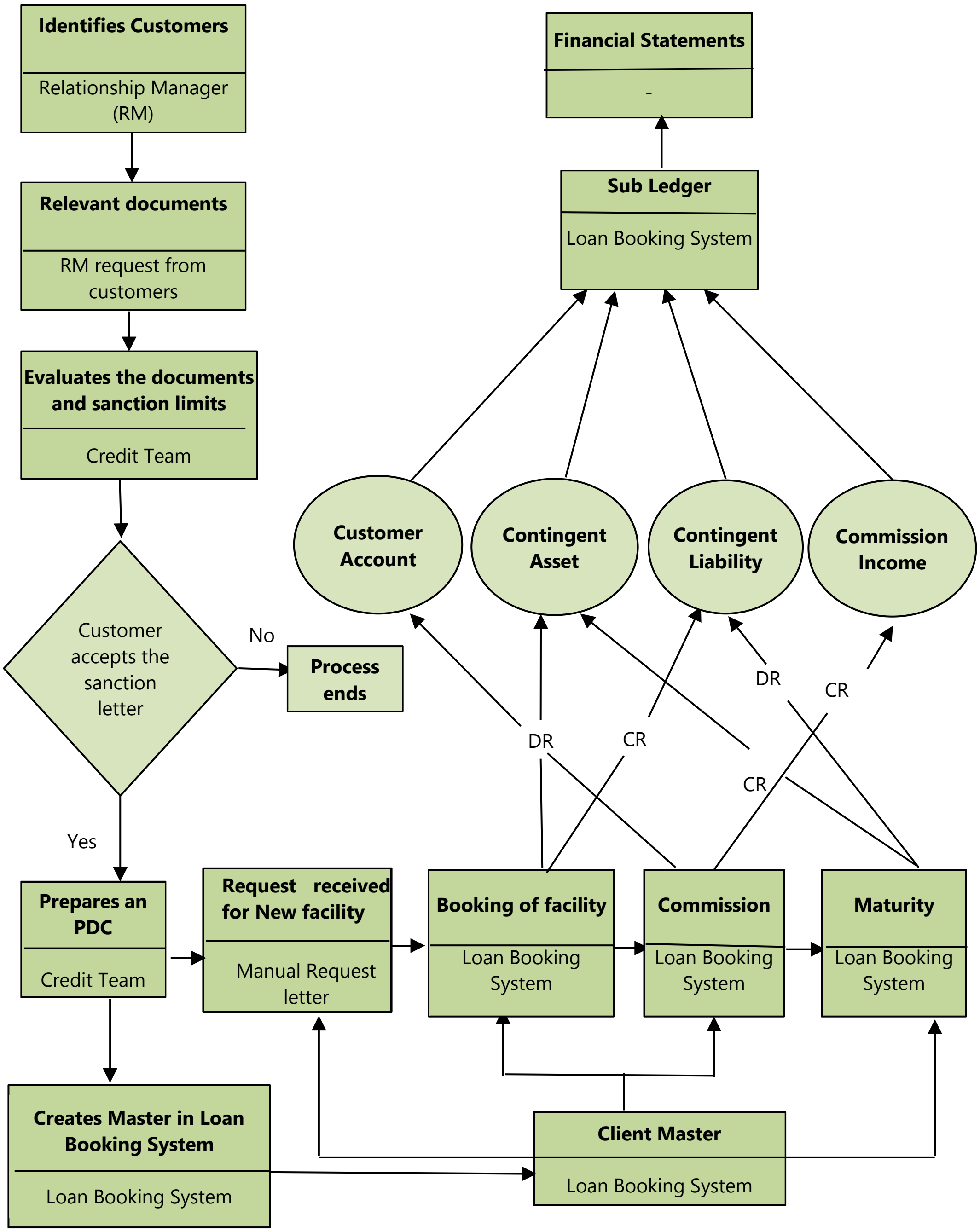


Fig. 5.3.7: Process Flow for Non - Fund based Loans

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

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

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

5.4 REPORTING SYSTEMS AND MIS, DATA ANALYTICS AND BUSINESS INTELLIGENCE

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

Risk Prediction for Basel III, based on Artificial Intelligence

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

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

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

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

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

5.5 APPLICABLE REGULATORY AND COMPLIANCE REQUIREMENTS

5.5.1 Impact of Technology in Banking

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

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

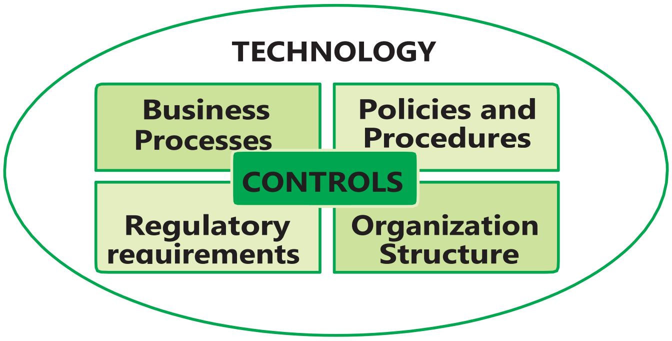


Fig. 5.5.1: Technology and Business Process Components

5.5.2 Money Laundering

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

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

1. Placement

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

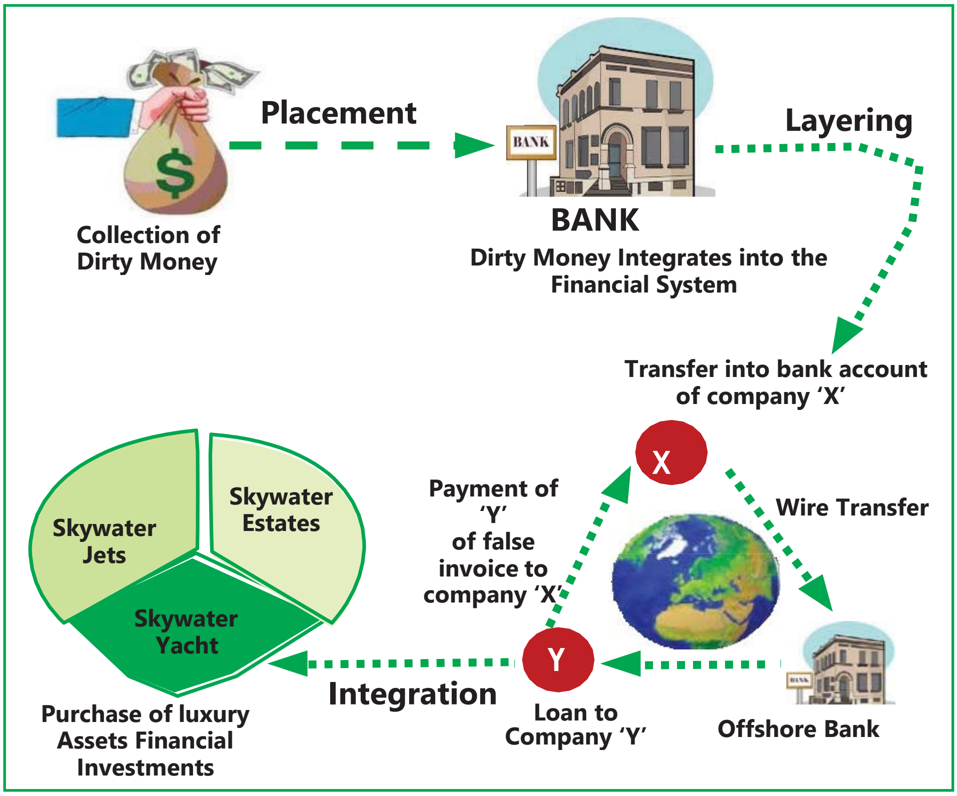

Placement
Collection of Dirty Money
BANK
BANK
Dirty Money Integrates into the Financial System
Layering
Transfer into bank account of company 'X'
X
Wire Transfer
Offshore Bank
Y
Loan to Company 'Y'
Payment of 'Y' of false invoice to company 'X'
Integration
Skywater Jets
Skywater Estates
Skywater Yacht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

Fig. 5.5.2: Money Laundering Process

2. Layering

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

3. Integration

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

II. Anti-Money laundering (AML) using Technology

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

III. Financing of Terrorism

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

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

5.5.3 Cyber Crimes

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

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

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

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

5.5.4 Banking Regulation Acts

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

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

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

I. Negotiable Instruments Act-1881 (NI Act)

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

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

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

II. RBI Regulations

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

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

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

III. Prevention of Money Laundering Act (PMLA)

Only relevant sections pertaining to the topic are discussed below:

CHAPTER II OFFENCE OF MONEY-LAUNDERING

Section 3. Offence of money-laundering

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

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

CHAPTER IV OBLIGATIONS OF BANKING COMPANIES, FINANCIAL INSTITUTIONS AND INTERMEDIARIES

Section 12. Reporting entity to maintain records.

(1) Every reporting entity shall—

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

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

(c) Omitted

(d) Omitted

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

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

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

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

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

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

Section 13. Powers of Director to impose fine.

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

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

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

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

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

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

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

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

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

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

CHAPTER X MISCELLANEOUS

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

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

***(2)** If any person -*

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

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

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

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

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

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

***Section 70. Offences by companies*.**

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

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

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

***Explanation 1 -* For the purposes of this section -**

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

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

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

II. Information Technology Act

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

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

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

<u>Some Definitions in IT Act</u>

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

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

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

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

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

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

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

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

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

A. Key Provisions of IT Act

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

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

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

(a) accesses or secures access to such computer, computer system or computer network 1[or computer resource];

(b) downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under;

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network;

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

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

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

Explanation - For the purposes of this section -

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

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

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

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

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

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

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

Section 43A: Compensation for failure to protect data.

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

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

Explanation - For the purposes of this section -

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

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

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

Section 65: Tampering with Computer Source Documents

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

Section 66: Computer Related Offences

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

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

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

Section 66-C: Punishment for identity theft

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

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

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

Section 66-E: Punishment for violation of privacy

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

B. Sensitive Personal Data Information (SPDI)

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

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

C. Privacy Policy

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

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

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

SUMMARY

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

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

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

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

TEST YOUR KNOWLEDGE

Theoretical Questions

1. Distinguish between Application Server and Database Server.

   Refer Section 5.2.2.

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

3. Briefly explain major components of a CBS solution.

   Refer Section 5.2.1.

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

5. What are the risks associated with CBS software?

   Refer Section 5.3.1.

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

   Refer Section 5.5.4.

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

   Refer Section 5.5.2.

Multiple Choice Questions

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

   (a) Advances

   (b) Letters of Credit

   (c) Reporting

   (d) Deposits

2. Which of the following is an application control?

   (a) Configuring system software

   (b) Setting parameters in masters

   (c) Transaction Logging

   (d) Back up of data

3. Which of the following is a General control?

   (a) Setting Database Security

   (b) Edit checks

   (c) Completeness check

   (d) Format check

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

   (a) On-line real-time processing

   (b) Transactions are posted in batches

   (c) Databases are maintained as per branch

   (d) Loan processing is done at branch

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

   (a) All computer errors are prevented

   (b) Frauds are detecting pro-actively

   (c) Undesired events are prevented or detected and corrected

   (d) Revenue targets are achieved

6. Which of the following best defines a risk?

   (a) Undesired events are prevented

   (b) Inherent vulnerabilities are identified

   (c) Physical threats are documented

   (d) Threat exploits vulnerability

7. Which of the following best defines Money Laundering?

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

(b) Tax Planning as per provision of IT Act

(c) Gifting immoveable property to relatives

(d) Transferring fixed deposit to employees

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

(a) Identify theft

(b) Stealing of mobile

(c) Stealing computer resource

(d) Violation of privacy

9. What is the primary objective of SPDI?

(a) Protecting computer software

(b) Securing critical information

(c) Securing Personal Information

(d) Identifying sensitive information

10. Which of the following is a cybercrime?

(a) Breaking into ATM

(b) Physical theft at branch

(c) Software piracy

(d) Altering name in demand draft

Answers

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

REFERENCES

BOOKS

1. Ron Weber, 'Information Systems Control and Audit', Pearson Education, Third impression, 2009

2. Kenneth C. Laudon, Jane P. Laudon & Rajanish Dass, 'Management Information Systems', Pearson, 11th Edition, Third Impression, 2011

3. James A Hall, 'Accounting Information Systems', South-Western College Publishing, 7th Edition, 2012

4. Sandra Senft and Frederick Gallegos, 'Information Technology Control and Audit', CRC Press, Third edition, 2009

5. Jake Kouns & Daniel Minoli, 'Information Technology Risk Management in Enterprise Environments', John Wiley & Sons, 2010

6. 'CISA Review Manual 2012', Published by: ISACA, 2011

7. Thomas F. Wallace and Michael H. Kremzar, 'ERP: Making It Happen: The Implementers' Guide to Success with Enterprise Resource Planning'

8. A Guide to ERP Benefits, Implementation and Trends by Prof Dr. LinekeSneller RC

9. Concepts in Enterprise Resource Planning by Ellen Monk and Bret Wagner

10. Integrated Auditing of ERP Systems by Yusufali F. Musaji

11. Adarsh,'XBRL for Indian CA'

12. Pat Mansel,'MIS 100 Success Secrets'

13. Jake Kouns and Daniel Minoli, 'Information Technology Risk Management in Enterprise Environments', Wiley.

14. ICAI Manual on Concurrent Audit of Banks (2016 Edition)

15. 2017 ICAI Guidance Note on Audit of Banks released by Auditing and Assurance Standards Board

16. ICAI - Standard on Auditing (SA) 315, Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and Its Environment

17. Erik Brynjolfsson, "The Productivity Paradox of Information Technology: Review and Assessment." Communications of the ACM, December, 1993.

18. Castells, Manuel. The Rise of the Network Society. 2nd ed. Cambridge, MA: Blackwell Publishers, 2000.

19. Valacich, Joseph, and Christoph Schneider. Information Systems Today: Managing in the Digital World. 4th ed. Upper Saddle River, NJ: Prentice-Hall, 2010.

20. Chui, Michael, Markus Loffler, and Roger Roberts. 'The Internet of Things.' McKinsey Quarterly, March 2010.

21. Gallagher, Sean, 'Born to Be Breached: The Worst Passwords Are Still the Most Common', Arstechnica, 2012.

22. Guel, Michele D, 'A Short Primer for Developing Security Policies', SANS Institute, 2007.

23. McAfee, Andrew and Erik Brynjolfsson. 'Investing in the IT That Makes a Competitive Difference.' Harvard Business Review, July-August, 2008.

24. McCallister, Erika, Tim Grance, and Karen Scarfone, 'Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)'.

25. National Institute of Standards and Technology, US Department of Commerce Special Publication 800-122, April 2010.

26. ERP Demystified, Second Edition by Alexis Leon

27. K Chandrasekaran, Essentials of Cloud Computing, CRC Press

WEB RESOURCES

1. www.isaca.org

2. www.itgi.org

3. www.ifac.org

4. www.iasb.org

5. www.cert-in.org.in

6. www.nist.org

7. www.rbi.org.in

8. www.sebi.gov.in

9. www.irda.giv.in

10. www.deity.gov.in

11. www.icai.org

12. www.inacle.com

13. www.tcs.com

14. www.ibm.com

15. www.mca.org.in

16. www.meity.gov.in

17. www.technopedia.com

18. www.zdnet.com

19. www.wns.com

20. www.csrc.nist.gov

21. www.deloitte.com

22. https://www.tutorialspoint.com

Glossary

A

- **Access Control** defines allowing / disallowing facilities and features in a software to a particular person or group of persons.
- **Accounting Master Data** is master data relating to financial accounting, e.g. ledger, Group, Cost Centre, etc.
- **Application Controls** are the controls which are implemented in an application to prevent or detect and correct errors. These controls -in-built in the application software ensure accurate and reliable processing.
- **Application Server** performs necessary operations and this updates the account of the customer
- **Artificial Intelligence** is defined as the capability of humans analyzing situations, create rules and ensure compliance with the rules is defined as intelligence. The same being done by system is called as Artificial Intelligence.

B

- **Back End** is a part of overall software system which does not interact with user directly and used to store data.
- **BHIM (Bharat Interface for Money)** is a Mobile App developed by National Payments Corporation of India (NPCI) based on UPI. It facilitates e-payments directly through banks and supports all Indian banks which use that platform.
- **Business Intelligence** provides tools for using data about yesterday and today to make better decisions about tomorrow.
- **Business Process Automation (BPA)** is the technology-enabled automation of activities or services that accomplish a specific function and can be implemented for many different functions of company activities.
- **Business Process** is an activity or set of activities that will accomplish a specific organizational goal.

C

- **Central Database** is a common database used by all the departments and business functions.

- **Computerized Accounting** is an accounting done using a computer software system.
- **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.
- **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.
- **Corporate Governance** is the framework of rules and practices by which a board of directors ensures accountability, fairness, and transparency in a company's relationship with its all stakeholders (financiers, customers, management, employees, government, and the community).
- **Corrective Control** is designed to correct errors or irregularities that have been detected.
- **Cybercrimes** are the 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.

D

- **Data Analysis** is defined as the science of examining raw data with the purpose of drawing conclusions about that information.
- **Data Flow Diagrams (DFD)** show the flow of data or information from one place to another. DFDs describe the processes showing how these processes link together through data stores and how the processes relate to the users and the outside world.
- **Data** is defined as a raw or unprocessed information.
- Database is the place where data is stored in a systematic and logical format, generally in tables and in rows and columns.
- **Detective Control** is designed to detect errors or irregularities that may have occurred.

E

- **E-commerce** refers to the products / Services being purchased and sold through electronic mode by using internet on desktops / laptops etc.
- **Electronic Safety** is making data safe using electronic methods like password protection.
- **Emerging Technology** are technology frontiers which are changing the way humans work and use technology.
- **Enterprise Information Systems** provide a technology platform that enables organizations to integrate and coordinate their business processes on a robust foundation.
- **ERP (Enterprise Resource Planning)** is a type of software system which take care of all the departments and functions.
- **E-wallets** are like normal wallet holding cash of owner, the only difference is that cash is not physical by e-form.

F

- **Financial Risk** is a risk that could result in a negative financial impact to the organization (waste or loss of assets).
- **Flowcharts** are used in designing and documenting simple processes or programs.
- **Front End** is defined as a part of overall software system which interacts with users directly and sends and receives data from database.

G

- **General Controls** also, known as infrastructure controls are applied to all systems components, processes, and data for a given organization or systems environment.

H

- **Hand held Devices** can be carried comfortably by user from one location to other like mobiles, IPAD etc. and are internet ready.
- **Human Resource** refers to the human being working in an organization, and are considered as resource for generating income.

I

- **Immediate Payment Service (IMPS)** is an instant interbank electronic fund transfer service through mobile phones. It is also being extended through other channels such as ATM, Internet Banking, etc.
- **Information** is the processed data.
- **Information Technology Act** provides the legal framework for electronic governance by **giving** recognition to electronic records and digital signatures. It also deals with cybercrime and facilitates electronic commerce.
- **Installed Application** are software application installed on the hard disc of computer of a user.
- **Integrated Systems** are the systems taking care of communication and data needs of all the departments and business functions.
- **Internal Control** is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the effectiveness and efficiency of operations, reliability of reporting and compliance with applicable laws and regulations.
- **Internet of Things** refers to the capability of household devices to communicate through internet.
- **Interoperability** is an ability of two or more applications that are required to support a business need to work together by sharing data and other business-related resources.
- **Inventory** is defined as a list of stock items intended for sale or consumption in normal course of business.
- **Inventory Master Data** is the master data relating to inventory accounting, e.g. Stock Items, Stock Groups, Godowns, Units of Measures, etc.
- **IT Control objectives** are a statement of the desired result or purpose to be achieved by implementing control procedures within a particular IT activity.

K

- **Knowledge** is defined as processed information derived from the raw data after processing. It is the inference out of information.

M

- **Machine Learning** refers to the application of Artificial Intelligence principles to help system improve their decision-making capabilities is Machine learning.
- **Management processes** measure, monitor and control activities related to business procedures and systems.
- **Master Data** is standing or relatively permanent data, not expected to change frequently.
- **M-commerce** refers to the Products / Services being purchased and sold through electronic mode with the help of accessing internet on hand held devices.
- **Mobile – App** is an application creating interface for user and vendors to interact.
- **Money Laundering** refers to 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’

N

- **Non-Integrated Systems** are the systems where separate database is maintained by each department.
- **Non-Master Data** is the Transaction data or data which is expected to change frequently.

O

- **Operational Processes** deal with the core business and value chain.
- **Operational Risk** is a risk that could prevent the organization from operating in the most effective and efficient manner or be disruptive to other operations.

P

- **Payment Gateway** is a way user / customers makes payment for an e-commerce/ m-commerce transaction.
- **Payroll Master Data** is the master data relating to payroll, i.e. Employee Names, Pay Heads, Salary Structure, Leave Types, etc.
- **Personal Information** is provided by customer such as name, address, phone number, and email, etc.

- **Physical Safety** ensures the safety of assets physically, e.g. locking the server room, controlling physical access to data.
- **Preventive Control** is designed to keep errors or irregularities from happening.
- **Process** is defined as the sequence of events or steps that uses inputs to produce outputs

R

- **Regulatory (Compliance) Risk** is a risk that could expose the organization to fines and penalties from a regulatory agency due to non-compliance with laws and regulations.
- **Report** is the information presented in a proper format.
- **Reputational Risk** is a risk that could expose the organization to negative publicity.
- **Risk Analysis** is the process of identifying security risks and determining their magnitude and impact on an organization. Information systems can generate many direct and indirect risks.
- **Risk** is any event that may result in a significant deviation from a planned objective resulting in an unwanted negative consequence. It is the potential harm caused if a threat exploits a vulnerability to cause damage to an asset.

S

- **Server** is a sophisticated computer that accepts service requests from different machines called clients.
- **Software Application** is a computer program designed to perform a group of coordinated functions, tasks, or activities for the benefit of the user.
- **Statutory** is related to statute or law.
- **Statutory Master Data** is master data relating to statute or law, e.g. Rates of taxes, forms, nature of payments, tax heads.
- **Strategic Risk** is a risk that would prevent an organization from accomplishing its objectives (meeting its goals).
- **Supporting processes** back core processes and functions within an organization.

- **System** is defined as a set of things working together as parts of a mechanism or an interconnecting network; a complex whole.

T

- **Transaction** is a give and take, exchange of benefits.

U

- **Unified Payment Interface (UPI)** is a system that powers multiple bank accounts (of participating banks), several banking services features like fund transfer, and merchant payments in a single mobile application.
- **User** is a person using a software programme.

V

- **Validation** is the checking of data input by the user for correctness, e.g. Mobile number must contain 10 digits.
- **Voucher** is a documentary evidence of transaction. A format of data entry for a transaction.
- **Voucher Type** are the types of voucher, e.g. Sales, Purchase, Receipt, Payment, Contra, Journal.

W

- **Web Application** are the software application installed on a website and access through a browser application.