Management Information And Control Systems

Notes

Ranjith Jayadevan

Feedback: rjwarrier@gmail.com

Contents

CHAPTER 1

BASIC CONCEPTS OF SYSTEMS

SYSTEM

- The term system can be defined as a set of interrelated elements that operate collectively to accomplish some common purpose or goal
- A system can be described by specifying its parts, the way in which they are related, and the goals which they are expected to achieve.
- Systems can be **abstract** or **physical**.
- An **abstract** system is an orderly arrangement of independent constructs.
- A **physical** system is a set of elements which operate together to accomplish an objective. E.g. Transportation system, computer system. Physical systems are more than conceptual construct, they display activity ore behavior. The parts interact to achieve an objective.

GENERAL MODEL OF A SYSTEM

(A) SIMPLE SYSTEM MODEL

INPUT----------→ PROCESS----------→OUTPUT

(B) SYSTEM WITH MULTIPLE INPUTS AND OUTPUTS

INPUT 1----------→ ----------→OUTPUT 1
INPUT 2----------→ **PROCESS** ----------→OUTPUT 2
INPUT 3----------→ ----------→OUTPUT 3

SYSTEM ENVIRONMENT

- All systems function within some sort of environment which surround the system and often interact with it.

- For any given problem there are many types of systems and many types of environments.

- **BOUNDARY** → The feature that defines and delineates a system forms its boundary. The system is inside the boundary and the environment is outside it.
- **SUB SYSTEM** → A subsystem is a part of a larger system. Each system is composed of subsystems which in turn are made up of other subsystems, having own boundaries.

- The interconnections and interactions between subsystems are called **INTERFACES.** They occur at boundary and take the forms of inputs and outputs.

- **SUPRA- SYSTEMS** → it refers to the entity formed by a system and other equivalent systems with which it interacts.

TYPES OF SYSTEMS

1. DETERMINISTIC SYSTEM

It operates in a predictable manner. The interaction among the parts is known with certainty. In a deterministic system one can accurately describe:

(a) state of the system at given point of time,
(b) its operation, and
(c) the next state of the system

2. PROBABILISTIC SYSTEM

It can be described in terms of probable behavior, but a certain degree of error is always attached to the prediction of what the system will do.

3. CLOSED SYSTEM

A closed system is self contained and does not interact or make exchange across its boundaries with its environment. Since they are isolated, they don't get feedback from the environment and tend to deteriorate.

→ **Relatively Closed System**

A relatively closed system is one that has only controlled and well defined inputs and outputs. It is NOT subject to disturbances from outside the system. They are relatively isolated from the environment, but not completely closed in physical sense.

4. OPEN SYSTEMS

They actively interact with other systems and establish exchange relationship. They tend to have form and structure to allow them to adapt to changes in their external environment for survival and growth.

SUB SYSTEMS

DECOMPOSITION >

- → To understand a complex system in a better manner, it is decomposed/ factored into subsystems. The boundaries and interfaces are also defined.
- → Such process is continued till smallest subsystems are of manageable size.
- → The subsystems resulting from this process generally form hierarchical structures.
- → In such a hierarchy, a subsystem is one element of supra system (i.e. The level before it)
- → Decomposition into the subsystems is used to analyze an existing system and/or to design and implement a new system.
- → The general principle in decomposition (which assumes that system objects dictate the process) is:-

  FUNCTIONAL COHESION>Components are considered to be a part of the same system if they perform or are related to the same function. The boundary then needs to be clearly specified, interfaces simplified and appropriate connections established among the subsystems.

SIMPLIFICATION >

- → It's the process of organizing subsystems so as to reduce the number of interconnections. **Clusters** of subsystems are established which interact with each other. Then a single interface path is defined from one cluster to other subsystems or cluster

PREVENTING SYSTEM ENTROPY >

System entropy > an increase in entropy takes place when a system run down and decay or become disordered or disorganized. Preventing or offsetting the increase of entropy requires input of matter and energy to repair, replenish and maintain the system. The maintenance of input is called "Negative Entropy".

SYSTEM STRESS AND SYSTEM CHANGE

→ System change when they undergo stress.

→ Stress is a force transmitted by the system's supra system that causes the system to change, so that the supra system can better achieve its goals.

→ **TYPES OF STRESS**

1. A change in the goal set for the system
2. A change in the achievement levels desired for existing goals.

These stresses can be applied separately or concurrently.

→ **CONSEQUENCES OF STRESS**

When a supra system exerts stress on a system,

(a) It will change to accommodate the stress, or

(b) It will decay and terminate

→ **PROCESS OF ADAPTATION**

Systems accommodate change either through a **Structural Change** or through a **Process Change.**

It is likely that those responsible for change will attempt to localize it by confining the adjustment process to only one or some of its subsystems instead of making global changes to structure and process of the system.

INFORMATION

- Information is "*Data that has been processed into a form that is meaningful to the recipient and is of real or perceived value in current or progressive decision"*
- Information is the substance on which business decisions are based. Therefore the quality of the information determines the quality and effectiveness of action/decision. This principle is known as GIGO i.e. Garbage In, Garbage Out.
- **CHARACTERISTICS OF INFORMATION**

1. **TIMELINESS:** Information to be of any use has to be timely.
2. **PURPOSE:** Information must have a purpose at the time it is transmitted. The basic purpose of information is to inform, evaluate, persuade and organize.
3. **MODE AND FORMAT:** Format of information should be so designed that it assists in-
   - decision making,
   - solving problems,
   - initiating planning,
   - controlling, and
   - Searching.

Reports should be supplied on an exception basis. Data should be classified into those groups which have relevance to problem at hand. It should be simple, relevant and highlight important points.

4. **REDUNDANCY:** It means the excess of information carried per unit of data. In a business situation redundancy maybe sometimes necessary to safeguard against error in communication process.
5. **RATE:** The rate of transmission/reception of information maybe represented by the time required to understand a particular situation.
6. **FREQUENCY:** Frequency with which information is transmitted or received affects its value.
7. **COMPLETENESS:** Information should be as complete as possible.
8. **RELIABILITY:** information should have an indication of confidence level.
9. **COST BENEFIT ANALYSIS:** The benefits that are arrived or derived from the information must justify the cost incurred in procuring information. Costs can be easily determined. But assessment of benefits is very subjective and its conversion into objective units of measurement is impossible. So to bypass this problem, managerial statements are classified into following **categories** with ref. to the **degree of importance** attached:
    (a) Absolutely essential Statements
    (b) Necessary statements
    (c) Normal statements, and
    (d) Extra statements.
10. **VALIDITY:** It measures the closeness of the information to the purpose which it purports to serve. The measure suiting the organization may have to be carefully selected and evolved.
11. **QUALITY:** Quality refers to correctness of information. Information is likely to be spoiled by personal bias. Errors maybe the **result** of :
    I. in correct data measurement and calculation methods
    II. failure to follow processing procedure
    III. Loss or no processing of data.

    To get rid of errors, internal controls should be developed and procedure for measurement prescribed.

VALUE OF INFORMATION

It is defined as the "*difference between the values of change in decision behaviors caused by the information and the cost of the information*". From a possible set of decisions, a decision maker will select one on the basis of information at hand.

BUSINESS INFORMATION SYSTEMS

A business is also a system. A business system depends on an abstract entity called the "*information system*". It is the means by which data flows from one person or department to another person or department. It serves all the systems of business, linking the different components in such a way that they effectively work towards same purpose.

The **purposes** of business information system are to:

1. process input
2. maintain files of data about the organization, and
3. Produce information, reports and other outputs.

The particular set of subsystems used – the specific equipments, programs, files and procedures constitute an **information system application.**

CATEGORIES OF BUSINESS INFORMATION SYSTEMS

1. Transaction Processing Systems (TPS)

- This is the most fundamental, computer based system in an organization.
- Transaction processing systems are aimed at expatiating and improving the routine business activities that all organizations engage.
- Transaction processing systems, if computerized provide speed and accuracy and can be programmed to follow routine without any variance.
- Transaction processing systems are operation oriented.
- Transaction processing systems thus can handle routine tasks effectively and efficiently.

2. Management Information Systems (MIS)

- Management information system assists managers in decision making and problem solving.
- They use results produced by transaction processing systems and also other information systems.

3. Decision Support Systems (DSS)

- Decision support systems are aimed at assisting managers who are faced with unique, non recurring decision problems. In this case often the decision determines the kind of information required
- In an unstructured environment, it is difficult to identify information in advance.
- A decision support system should have therefore greater flexibility.

- A decision support system is of much more use when decisions are of an unstructured or semi structured nature. In this situation problem area can be modeled and various alternatives are explored.
- Decision support systems should be seen as an integrated piece of software incorporating database, model base and user interface.
- Decision support systems are used both at a tactical level and a strategic level.

4. Executive Information Systems (EIS)

- Executive information systems are designed primarily for the strategic level of the management.
- Executive information systems use high end graphical interfaces and multimedia technology to present information in summarized forms. They also use higher end computer systems which can interact with other systems both inside and outside the business.
- Executive information systems tend to be externally focused, strategically based systems using both internal and external data. Other computer based systems mainly concentrate on internal control aspects of the organization.

5. Expert Systems (ES)

- These are designed to replace human experts.
- They are important where expertise is scarce and expensive.
- Expert systems are not general.
- They have arisen largely from academic research into AI
- These would be of greater use in tactical and strategic level.

CHAPTER 2

TRANSACTION PROCESSING SYSTEMS

INTRODUCTION

Accounting information systems depend heavily on the flow of data through various organizational subsystems. Effective Transaction processing systems ensure the capture of appropriate data and accurate information reporting.

TRANSACTION PROCESSING CYCLE

- Accounting information systems includes the variety of activities associated with an organization's transaction processing cycle.
- A **Transaction processing cycle** organizes transactions by an organization's business processes, the nature and type of which may vary depending on the information needs of specific organization.
- However **FIVE** common transaction processing cycles can be formed based on transactions which are common to most business organizations.
    1. **Revenue Cycle >** This include events related to distribution of goods & services and collection of related payments.
    2. **Expenditure Cycle >** This include events related to the acquisition of goods & services and settlement of related obligations.
    3. **Production Cycle >** This include transformation of resources into goods and services.
    4. **Finance Cycle >** This include acquisition and management of capital funds including cash.
    5. **Financial Reporting Cycle >** Its not an operating cycle. It obtains accounting and operating data from other cycles and processes in such a manner that financial reports may be prepared.
- The **objective** of grouping transactions is to **cluster** these transactions together in a way that **simplifies** information processing.
- A transaction processing cycle consists of one ore more **Application Systems.**
- An application System processes logically related transactions.

Commonly included Application Systems in each transaction processing cycle

REVENUE CYCLE	EXPENDITURE CYCLE	PRODUCTION CYCLE	FINANCE CYCLE
> Customer Order Entry	> Vendor Selection	> Production Control	> Cash Management and Control
> Billing	> Requisitioning	> Product Costing	> Debt Management
> Accounts Receivable	> Purchasing	> Inventory Control	
	> Accounts Payable		> Administration of employees welfare plans
> Sales Reporting	> Payroll	> Property Accounting	

- **BENEFITS OF TRANSACTION PROCESSING CYCLE**

1. Transaction processing cycle concept provides a framework for analyzing an organization's activities.
2. It also provides a basis for categorizing the flow of economic events that are common to all organizations.
3. Transaction processing cycle offer a systematic framework for the analysis and design of Accounting Information System.

COMPONENTS OF TRANSACTION PROCESSING SYSTEMS

The principal components of a transaction processing system are:-

1. Inputs,
2. Processing,
3. Storage, and
4. Output.

These can be part of either a manual or/and computerized system.

1. INPUT → Source Documents are the physical evidence of inputs to transaction processing systems. They serve several purposes.

+ PURPOSES OF SOURCE DOCUMENTS

- ➔ Capture Data
- ➔ Facilitate Operation (by communicating data & authorizing operation in the process).
- ➔ Standardize Operation (by indicating what data required & what actions need to be taken).
- ➔ Provide a permanent file for future analysis.

+ FORMAT OF SOURCE DOCUMENTS

- ➔ Easy to read and understand.
- ➔ Serve to collect & distribute information.
- ➔ Establish authenticity or authorization.
- ➔ Capable of capturing accurate data.

2. PROCESSING → This involves the use of journals and registers to provide a permanent and chronological record of inputs. Entries are made either manually or by computers.

+ Journals > Journals are used to record financial & accounting transactions. They are used to provide a chronological record of financial transactions. However its often practically impossible to record all transactions in a single Day book. So **Special Journals**

are used to record similar and recurring transactions in conjunction with a separate General Ledger. Examples of Special Journals are:-

- ☞ Sales Journal
- ☞ Cash Receipt Journal.

The design of Special Journals is one of the most important step in the design of AIS.

3. STORAGE → Ledgers and files provide storage of data in both manual and computerized systems. The general ledger, the accounts/ vouchers payable ledger and the accounts receivable ledger are the records of financial account.

+ Computer Storage: Types of Files

A file is an organized collection of data. There are 2 types of files:-

- ➔ **Transaction File |** It's a collection of transactions and input data and usually contain data that are temporary, so management's interest in these files is also temporary.
- ➔ **Master File |** It's a collection of data that are of amore permanent or continuing interest.

4. OUTPUTS → Any document generated in the transaction processing systems is an output. Common outputs of a transaction processing systems are:-

+Trial Balance

+Financial Reports – Balance Sheet and Profit & Loss Account

+Operational Reports – Summarize the results of transaction processing in a statistical or comparative format.

+Pay Cheques

+Bills of Lading

+Voucher Cheques

The nature and content of such reports depend on the nature of a firm and its transaction processing activities.

→ COMPUTER PROCESSING

When computers are used for processing two different modes of processing can be used:

1. **Batch Processing:** Batches of transactions are accumulated as a transaction file which is subsequently posted to ledgers by computer programs. The ledgers are then periodically processed to generate financial statements.
2. **Direct Processing:** Individual transactions are posted directly to ledgers rather than being batched to build a transaction file.

A Reference/Table File contains data that are necessary to support data processing.

DESIGN OF ACCOUNTING INFORMATION SYSTEMS

- ➔ When planning a new system, the developers usually start by designing the outputs of the system.
- ➔ Outputs then drive the inputs to Accounting information systems.
- ➔ Source documents are then designed in such a way that those are easy to use and can capture accurate data.
- ➔ To increase the effectiveness of a transaction processing system, accounting data is **coded** to identify accounting information uniquely.

➔ **Uses Of Codes**

(a) To identify accounting information uniquely,
(b) To compress data,
(c) To classify transactions in accounts, and
(d) To convey special meanings.

➔ **Types of Codes**

(1) Mnemonic Codes
(2) Sequence codes
(3) Block codes, and
(4) Group codes

➔ **Factors influencing Code Selection and Design**

(1) The code's use
(2) The need of consistency
(3) Considerations of design efficiency
(4) An allowance for growth, and
(5) The desire to use standard codes throughout a company.

**

CHAPTER 3

MANAGEMENT INFORMATION SYSTEMS

INTRODUCTION

Management information system deals with information, which is critical for the success of any business organization. Management information system is used by managers as a means for better management and scientific decision making. Right information is needed by managers for executing important managerial functions like planning, organizing staffing, directing and controlling. Management information system is a special system instituted to ensure the flow of correct information at regular intervals to various hierarchical management levels.

CONCEPTS OF MANAGEMENT INFORMATION SYSTEM

→ **MIS** | MIS consists of three terms viz management, information and system. The concept of Management information system is better understood if each element of term Management information system is defined **separately.**

➔ **MANAGEMENT |**

Management refers to a set of **functions and processes** designed to initiate and co ordinate group efforts in an organized setting **directed** towards

- ☞ promotion of certain interest,
- ☞ preserving certain values, and
- ☞ pursuing certain goals,

And involves,

- ☞ mobilization
- ☞ combination
- ☞ allocation, and
- ☞ utilization

Of physical, human and other needed resources in a **judicious** manner by employing appropriate skills, approaches and techniques.

+ Activities Performed By Managers

1. Determination of organizational objectives and developing plans to achieve them.
2. Securing and organizing the human and physical resources (to achieve the objectives).
3. Exercising adequate control over these functions.
4. Monitoring the results.

➔ **INFORMATION |**

Information is data that have been put into a meaningful and useful context.

➔ **SYSTEM |**

System is a composite entity consisting of a number of elements which are independent and interacting, operating together for the achievement of an objective.

MANAGEMENT INFORMATION SYSTEM

MIS is a network of information that **supports** management **decision making.** The role of MIS is to recognize **information** as a **resource** and then using that resource for effective and better achievement of organizational objectives.

Definition of MIS

By Canith > An approach that visualizes the business organization as a single entity composed of various inter related and inter dependent sub systems looking together to provide **timely and accurate** information for management **decision making** which leads to optimization of overall enterprise goals.

By GB Davis > An integrated man/machine system for providing information to support the operations, management and decision making functions in an organization.

A management information system:-

1. Applies to all management levels,
2. Linked to all organizational sub systems
3. Functions to measure performance, monitor progress, evaluate alternatives or provide knowledge for change or collective action, and
4. Is flexible both internally and externally.

In short, MIS **aids management in making, carrying out and controlling decisions.**

CHARACTERISTICS OF AN EFFECTIVE MIS

1. **Management Oriented**
   First step in designing an MIS is an appraisal of management needs and overall business objectives. MIS should be able to satisfy information needs of top, middle and bottom levels of management.
2. **Management directed**
   Management should actively direct the systems development efforts as MIS is management oriented. Management should be responsible for setting system specifications and it must play a key role in subsequent trade off decisions that occur in system development.

3. **Integrated**
   Development of information should be an integrated one i.e. a complete look at inter locking sub systems that operate within a company. All functional and operational information sub systems should be tied together into one entity.
4. **Common data flows**
   It means use of common input, processing and output procedures and media whenever possible and desirable. Data analysts capture data as close as to its original source and then try to minimize data processing procedures and sub systems to process the captured data and also try to minimize no: of outputs. All this avoids unnecessary duplication of data.
5. **Heavy planning element**
   Since it takes longer for MIS to get established, designer should keep in mind future objectives and requirements of firm's information.
6. **Sub system concept**
   MIS should be broken down to digestible sub systems which can be implemented in phases.
7. **Common database**
   Database is *super file* which consolidates and integrates data records formerly stored in many separate data fields. Thus all the sub systems of MIS can access data from a common database.
8. **Computerized**
   Though MIS can be rum without using computers, use of computers increases the effectiveness of the systems.

MISCONCEPTIONS/MYTHS ABOUT MIS

1. **The Study of MIS is about use of computers.**
   MIS may or may not be computer based. Computer is just another tool used in management information system.
2. **More data in reports means more information for managers.**
   Its not quantity of data, but its relevance which is more important to managers in decision making process.
3. **Accuracy in reporting is of vital importance.**
   This is true at lower levels of management. But at higher levels, since decisions are based on principles and objectives, accuracy is relevant, but not ideal. A fairly correct representation is enough.

PRE REQUISITES OF AN EFFECTIVE MIS

1. **Database**

   A database is a super file which consolidates data records. Normally the database is sub divided into the major information subsets needed to run a business, which are:

   a) Customer and sales file
   b) Vendor file
   c) Personal file
   d) Inventory file, and
   e) General Ledger accounting file.

   - **Characteristics of Database**
     1. Each subsystem utilizes same data and information is kept in the same file to satisfy its information needs.
     2. User oriented.
     3. It's capable of being used as a common data source to various users.
     4. Available to authorized persons only.
     5. It's controlled by a separate authority, known as DBMS.

   - **Requirements of Database**
     1. Computer hardware
     2. Software
     3. Experienced computer professionals, and
     4. Good data collection systems.

2. **Qualified System and Management Staff**

   MIS should be manned by qualified officers who understand clearly the views of their fellow officers. For this the organization management base should comprise of two categories of officers viz.

   1. Systems and Computer Experts, and
   2. Management Experts

   - **Qualities of Personnel**
     1. They should have expertise in their respective area.
     2. They should be capable of understanding management concepts.
     3. They should be clear about processes of decision making and information requirements.
     4. Management experts should clearly understand functions of a computer.

   Problem: *This prerequisite has one main problem: acquisition and retention of qualified personnel is difficult.*

3. **Support of Top Management**

   Full support of top management is needed because:

   a. Subordinate managers are lethargic about activities which don't receive support of their superiors.
   b. The resources used in computer based information system are large.

4. **Control and Maintenance of MIS**

   Control means operation of a system as it was designed to operate. Management should device checks to find out whether users have created own procedures and shortcut which reduce effectiveness of management information system.

5. **Evaluation of MIS**

   Evaluation of MIS and taking appropriate action is required to ensure that MIS can satisfy information needs in future. However following points should be considered in the evaluation of MIS:

   1. Examining the flexibility of the system (to know whether it can cope with changes in information needs)
   2. Ascertaining views of users and designers of MIS about its capabilities and deficiencies.
   3. Guiding the appropriate authority about steps to be taken to maintain effectiveness of MIS.

CONSTRAINTS IN OPERATING MIS

SlNo	Constraint	Solution
1	Non availability of experts who can diagnose the objectives of the organization and provide desired direction for installing and operating the system.	By Grooming the internal staff
2	Experts face the problem of selecting the sub system of MIS to be installed and operated upon.	Need and importance of a function for which MIS can be installed first can be used as reference.
3	Non cooperation of staff	Educating the Staff
4	High turnover of MIS staff	Creating better working conditions
5	The approach for designing and implementing MIS is non standardized as it varies from entity to entity.	Industry standards can be set up
6	Difficulty in quantifying the benefits of MIS. So that a cost-benefit comparison is not possible	**---**

EFFECTS OF USING COMPUTER FOR MIS

1. **Speed of processing and retrieval of data increases.**
   Processing of data and retrieval of relevant information can be achieved extremely fast using a computer.

2. **Scope of use of information system has expanded.**
   Computers can be used to provide information to users sitting at a remote distance from a centrally located server using an online, real time system.

3. **Scope of analysis widened.**
   The use of computers can provide multiple type of information accurately to decision makers so that they can conduct a thorough analysis of the problems to arrive at a solution.

4. **Complexity of system design and operations increased.**
   The need for highly processed and sophisticated information based on multitudes of variables has made the designing of the system quite complex. The computer manufacturers have developed software to cater to the sophisticated needs of their customers.

5. **Integrates the working of different information sub systems.**
   A Management information system is generally a federation of sub systems. These subsystems are required to provide information to support operational control, management control and strategic planning. Such information may be made available from a common database.

6. **Increases the effectiveness of information sub system.**
   Computers can provide relevant information in time to personnel thus enabling them to take accurate decisions at relatively low cost.

7. **More comprehensive Information.**

LIMITATIONS OF MIS

1. The quality of output of MIS is often determined by the quantity of input and processes.
2. MIS is **not** a substitute for effective management as it cannot replace managerial judgment in decision making.
3. MIS may not have the requisite flexibility to update itself in an ever changing environment.
4. MIS may not provide tailor made information packages suitable for every type of decisions made.
5. MIS generally ignores qualitative data.
6. MIS is less useful for making non programmed decisions.

7. Effectiveness of MIS decreases if information is not shared within the organization.
8. MIS effectiveness decreases as a result of frequent changes in top management.

ESTABLISHING THE INFORMATION NEEDS IN MANAGEMENT PROCESS

- The establishment of information needs in management process means establishing of information requirement of its managers.
- This is usually performed by system analysts and systems designers.
- The planning information requirements of executives can be categorized into 3 broad categories:

(A) Environmental Information

1. Government Policies
2. Factors of Production – about source/cost/location etc of major factors of production.
3. Technological environment – about changes in technology.
4. Economic Trend

(B) Competitive Information

1. Industry demand
2. Firm demand
3. The competitive data

(C) Internal Information

1. Sales forecast
2. Financial plan/Budget
3. Supply factors
4. Policies

FACTORS ON WHICH INFORMATION REQUIREMENT DEPEND

1. Operational Function

➔ The grouping of several functional units on the basis of related activities into a sub system is termed as operational function. E.g.> Marketing

➔ Operational Functions differ in respect of content and characteristics of information required by them. The content of information depends upon the activities performed under an operational function.

2. Type of Decision making

➔ **Programmed Decisions**

- Programmed decisions refer to decisions made on problems and situations by reference to a pre determined set of precedents, procedures, techniques and rules.
- These are well structured in advance and are time tested for their validity.
- Programmed decisions are made with respect to familiar routine, recurring problems which are amenable for structured solution by application of known and well defined operating procedures and processes.
- Not much judgment and discretion is needed.
- They tend to be consistent over a period of time.

➔ **Non Programmed Decisions**

- These decisions are those which are made on situations and problems which are novel and non repetitive and about which not much knowledge and information are available.
- They are not made with reference to any predetermined guidelines, SOPs and rules, but by application of managerial judgment, Intelligence, Experience and Vision.
- These decisions generally deal with problems which arise infrequently and about which not much is not known.
- Solutions and decisions on such problems tend to be unique or unusual.

3. Level of Management Activity

➔ **Strategic Level**

- It's concerned with developing of organizational mission, objectives and strategies. Decisions made at this level of organization handle problems critical to the survival and success of the organization are called "Strategic Decisions"
- Strategic Decisions are made under conditions of partial knowledge or ignorance and in a way are comparable with non programmed decisions.

➔ **Tactical Level**

- At this level managers plan, organize, lead and control the activities of other managers. Tactical Decisions are made at this level to implement Strategic Decisions.
- Tactical Decisions are of relatively structured nature
- ***Characteristics of Tactical Decisions***
  1. Specific and Functional. They are made in a relatively closed setting
  2. Information for Tactical decisions is more easily available
  3. Decision variables can be forecast and quantified.
  4. These are made with a strategic focus.

➔ **Supervisory Level**

- At this level managers co ordinate the work of others who are not themselves managers.

LEVELS OF MANAGEMENT AND THEIR INFORMATION REQUIREMENT

1. **Strategic (Top) Level**
   - Top level is concerned with overall of designing, directing and managing the organization in an integrated manner.
   - This level consists of those executives whose responsibilities relate to the whole organization. They are accountable for the effectiveness and efficiency of the organization as a whole.
   - Top management's main responsibility is in the direction of determining the overall goals and objectives of the business.
   - It deals mainly with long term plans, policy matters, broad objectives and budget framework.

2. **Middle (Tactical) Level**
   - Middle level (Administrative Management) overlaps the Top and Supervisory levels of management.
   - It is responsible for the elaboration, classification and operation of organizational goals, strategies and policies in terms of action programs and norms of performance.
   - It's concerned with the task of formulating pragmatic operating policies and procedures for guidance of supervisory management.
   - Much of information used by Middle level managers are Internal in nature.

3. **Supervisory Level**
   - Supervisory level (Operations Management) is the team of management positions at the base of the hierarchy.
   - It's concerned with implementing operational plans, policies and procedures for purposes of conversion of inputs to outputs.
   - Managers are responsible for routine, day to day decisions which don't require much judgment and discretion.
   - It functions in a relatively closed environment.
   - It mostly requires internal information which is routine, structured, reliable and relatively complete.

INFORMATION REQUIREMENT AT VARIOUS LEVLES OF MANAGEMENT

INTERNAL INFORMATION	EXTERNAL INFORMATION
Top Levlel	
Historical- Sales and Cost Profit, Cash-flow, Sales, Expenses etc Financial ratios, interest, Credit outstanding Long term debt, deliquent accounts Progress report of Projects and Cost updates	Competitive activities Economic Trends Customer Preferences, style and changes Technological Changes, legal rulings
Middle Level	
Descriptive information Current performance indicators Over-Under budgets Historical profits, sales and income	Price changes, shortages Demand or supply Credit conditions
Supervisory Level	
Unit sales and expenses Current performance Shortages and bottle necks Operating efficiencies and inefficiencies Input-Output ratios Maintenance reports	Sensitive Changes affecting material Supplies and sales.

**

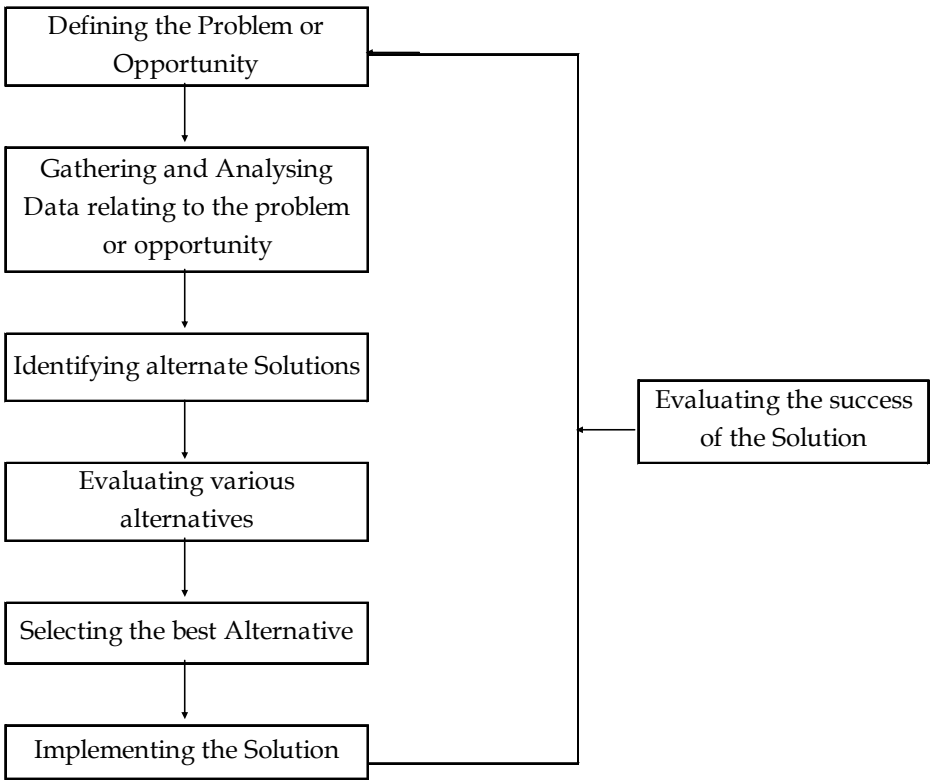
CHAPTER 4

SYSTEM APPROACH AND DECISION MAKING

SYSTEM APPROACH TO PROBLEM SOLVING | AN INTRODUCTION

- ➔ The System Approach visualizes an organization as group interacting and interdependent parts with a purpose.
- ➔ Each problem should be examined in its entirety to the extent possible and economically feasible from the point of view of the overall system of which the problem under consideration is one part.
- ➔ Manager should make conscious attempt to understand the relationship among various parts of the organization and their role in supporting the overall performance of the organization.
- ➔ Before attempting to solve any problem he should understand fully how the overall system would respond to changes in its component parts.
- ➔ A manager should view the organization as dynamic whole and he must anticipate the intended as well as unintended impacts of his decision.

SYSTEM APPROACH OF DECISION MAKING



DECISION MAKING IN MIS

➔ Decision making is the managerial process and function of choosing a particular course of action out of several alternative courses for the purpose of achieving the given goals.

➔ Its an important step towards reducing the gap between the existing situation and the desired situation through:

- Solving problems and crises
- Making use of opportunities
- Committing the organization to a specific course of action, and
- Commitment of resources in specific ways.

➔ Decision making underlies much of managerial activity in an organization. Decisions may be major or minor, strategic or operational.

➔ Managers manage by making decisions and getting them implemented in a systematic manner.

PERVASIVENESS OF DECISION MAKING

➔ Managers manage by making decisions and getting them implemented in a systematic manner.

➔ It's the responsibility of Top Management to create a decision making system as an integral part of the organizational system. This can be done through:

(a) proper delegation of authority
(b) installation of suitable information system
(c) formulation of organizational policies and procedures
(d) training of subordinate managers to improve their decision making and judgmental skills and
(e) Creation of an organizational climate conducive to making sound decisions.

➔ Decision making is integral to all the managerial processes from setting up goals and formulating strategies to leadership and communication.

➔ It runs through all managerial functions

➔ There is a close relationship among the decisions made performing the various managerial functions.

CLASSIFICATION OF DECISIONS

Decisions can be classified into following categories:

1. PROGRAMMED AND NON PROGRAMMED DECISIONS

➔ **Programmed Decisions**

- Programmed decisions refer to decisions made on problems and situations by reference to a pre determined set of precedents, procedures, techniques and rules.
- These are well structured in advance and are time tested for their validity.
- Programmed decisions are made with respect to familiar routine, recurring problems which are amenable for structured solution by application of known and well defined operating procedures and processes.
- Not much judgment and discretion is needed.
- They tend to be consistent over a period of time.

➔ **Non Programmed Decisions**

- These decisions are those which are made on situations and problems which are novel and non repetitive and about which not much knowledge and information are available.
- They are not made with reference to any predetermined guidelines, SOPs and rules, but by application of managerial judgment, Intelligence, Experience and Vision.
- These decisions generally deal with problems which arise infrequently and about which not much is not known.
- Solutions and decisions on such problems tend to be unique or unusual.

2. TACTICAL AND STRATEGIC DECISIONS

➔ **Strategic Decisions**

- It's concerned with developing of organizational mission, objectives and strategies. Decisions made at this level of organization handle problems critical to the survival and success of the organization are called "Strategic Decisions"
- Strategic Decisions are made under conditions of partial knowledge or ignorance and in a way are comparable with non programmed decisions.

➔ **Tactical Decisions**

- At this level managers plan, organize, lead and control the activities of other managers. Tactical Decisions are made at this level to implement Strategic Decisions.
- Tactical Decisions are of relatively structured nature
- ***Characteristics of Tactical Decisions***

1. Specific and Functional. They are made in a relatively closed setting
2. Information for Tactical decisions is more easily available
3. Decision variables can be forecast and quantified.
4. These are made with a strategic focus.

3. INDIVIDUAL AND GROUP DECISIONS

➔ **Individual Decisions**

- Many decisions, even critical ones in an organization are made by individual managers, who assume full responsibility for the consequences of such decisions.
- They may get information from various sources, discuss with subordinates etc but the responsibility and the authority of taking the decision vest with that particular person.

➔ **Group Decisions**

- Group decisions are those which are made by more than one manager.
- Problems, which have interdepartmental effects calls for such decisions.
- E.g.> Decisions of Board of Directors.

Group Decisions Vs Individual Decisions

☞ **Advantages of Group Decisions**

1. The decision making function and process get enriched by the pooling of diverse expertise, knowledge, authority and perspectives represented by the group.
2. Elaborate group deliberation and consideration of alternative courses from several angles tend to ensure that decisions of high quality are made.
3. It's more desirable to vest high degree of decision making authority in a group than in individual as individual may not be able to use it properly and fully.
4. Group decisions enjoy a high degree of acceptance and pragmatism.

☞ **Disadvantages of Group Decisions**

1. Delay in decision making.
2. Lack of conformity and responsibility among group members.
3. Dilution of the quality of decision by compromise and conformity among members of the group.

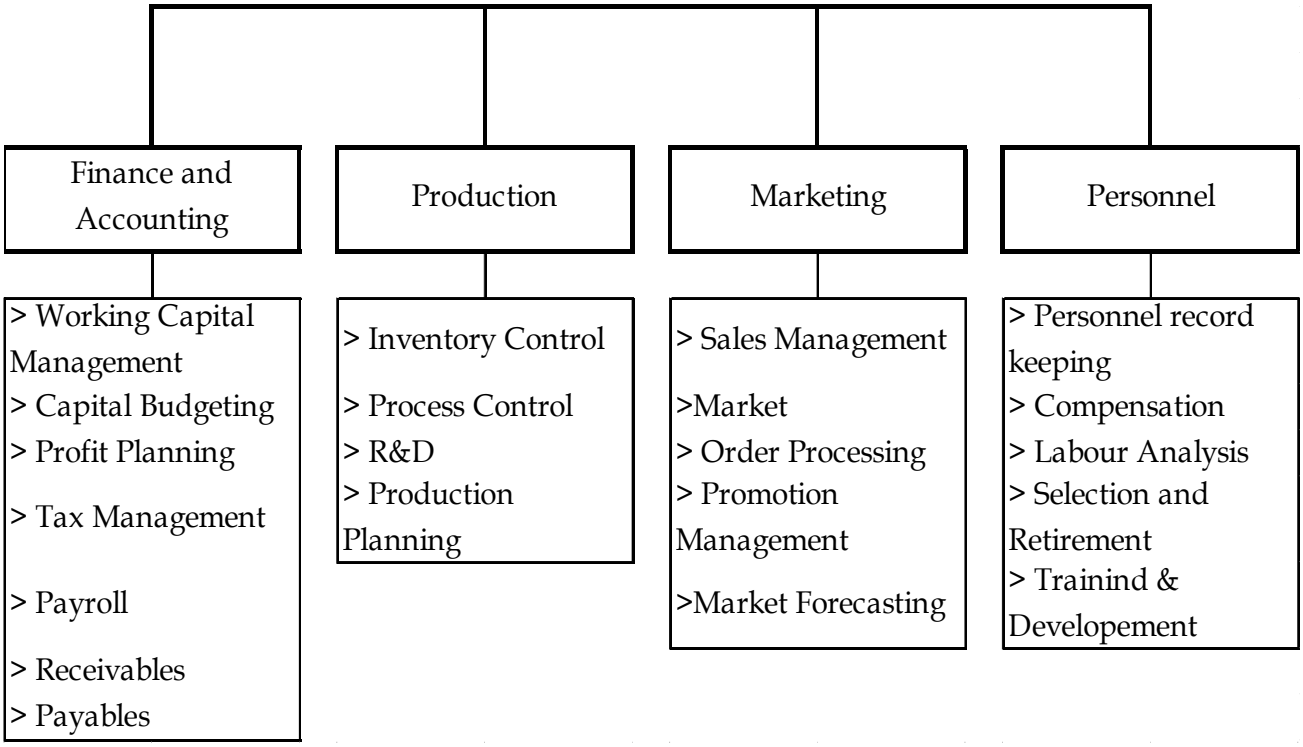
DECISION MAKING THROUGH (COMPUTERISED) MIS

- ➔ A growing no: of companies are using MIS in aiding decision making process.
- ➔ A computerized MIS can be used :
    1. Market Research > to simulate demand and assess companies potential for a share of market and profitability.
    2. To test the impact of strategies/ ideas on future profitability.
    3. Forecasting> to determine needs for funds and physical resources.
    4. Risk analysis.
    5. To understand key factors involved in implementing a new policy.
    6. Sensitivity analysis> measurement of effect of the variation of individual factors on final result.
- ➔ A computer based MIS puts pertinent information into a analytical framework that aids management decision making process.

FUNCTIONAL INFORMATION AREAS

- ➔ A business manager should have a general understanding of the major ways information system are used to support each of the functions of business.

Major Functional Information Areas



1. FINANCE AND ACCOUNTING SYSTEM

➔ Finance and accounting are separate functions. However they are closely related. Finance function ensures adequate organizational financing at low costs so as to maximize returns to share holders. Accounting involves classification of transactions and summarization into standardized statements.

➔ **Financial Decision Making**

- ♦ It deals with **procurement** of funds and their effective **utilization** properly and profitably in the business.
- ♦ Decisions are based on techniques such as Budgeting, risk analysis etc.

➔ **Financial Decisions**

1. Estimation of requirement of funds
2. Capital structure decisions- to select optimum mix
3. Capital budgeting decisions- analyzing feasibility of long term investments.
4. Profit planning- decisions concerning profit and dividends
5. Tax management- reducing tax payout by taking full advantage of exemptions, concessions etc.
6. Working capital management- concerned with effective financing of current assets.
7. Current asset management.

2. MARKETING SYSTEM

➔ Marketing system is aimed at supporting the

- ♦ decision making,
- ♦ reporting, and
- ♦ transaction processing requirements

Of marketing and sales management.

➔ The main **Objectives** marketing system are :

(a) to develop, promote, distribute sell and service the products of the organization ; and

(b) to return a profit that is enough to justify the existence of the organization.

➔ The marketing system is mainly concerned with Product Market Development by taking into account factors like product lifecycle, competitive trends, demand etc

➔ It's also concerned with sale of firms products to customers.

➔ The information that marketing management receives is important; however the information that marketing generates is vital to the rest of the organization. E.g. Sales forecasting affects production schedule.

➔ Because of this the impact of an ineffective Marketing Information System is felt throughout the organization as marketing is the company's only revenue generating branch.

➔ A well developed marketing information system can give a competitive advantage to the organization.

➔ **COMPONENTS OF MARKETING INFORMATION SYSTEM**

1. SALES

- The objective of the sales manager is to co ordinate the efforts so that the long term profitability of the company is maximized.
- Decisions require intensive interaction with market place and co ordination with logistical operations of inventory and production.
- **Sales Report >** A specialized sales support information system should provide information to sales personnel about the following:
    1. product description and performance specifications
    2. product prices
    3. sales promotion
    4. strengths and weaknesses of competitors' products
    5. inventory level , and
    6. Buying habits of consumers.

- **Sales Analysis** > The purpose is to provide information regarding :
    1. product sales trends
    2. Product profitability
    3. performance of each sales region and branch
    4. Performance of salespersons.
- Information for sales analysis is derived primarily from sales order entry system.
- Profitability reporting requires information about product administrative and selling costs.

2. MARKET RESEARCH AND INTELLIGENCE

- The objective of marketing research is to investigate problems confronting the other managers in the marketing function.
- For this marketing research dept. must either periodically or upon demand gather information from a wide variety of sources.
- Marketing research helps in following informational needs of managers:

1. information about the economy and economic trends,
2. information about past sales and sales trends
3. information about potential new markets for products
4. information about competitors, its products etc

- Market research differs from market intelligence as the former concentrates on the market place and the latter is concerned with only one aspect of market place : Competition.

3. ADVERTISING AND PROMOTION

- This involves planning and executing advertising campaigns and to carrying out various product promotions such as coupons, contests etc.
- Given a limited budget it has to allocate the funds among the various products, markets (locations) and media (modes).
- An advertising information system should continually update its information base on the basis of development in market place.

4. PRODUCT DEVELOPMENT AND PLANNING

- Product development involves:
  1. Analyzing a possible opportunity for a new product, and
  2. Evaluating preferred specifications and probable market success.
- Customer suggestions and reactions to existing products may help the management in identifying the need for a new product.
- The product development team uses information like customer suggestions, competition, and demand of other similar products etc to develop specifications of the new product.
- Product planning system provides marketing management with packaging, promotion, pricing and style recommendations throughout the life of the product.

5. PRODUCT PRICING SYSTEM

- Product pricing is a complex managerial activity that is affected by product costs, demand, competition, market psychology etc.
- Pricing decisions generally are affected by:
  - competition : price of competitors', their strategies etc; and
  - The margin the organization wants to maintain.
- Prices should be adjusted to changes in both marketplace and in the organization.

6. CUSTOMER SERVICE

- The main objective of marketing is to satisfy customers with the product by:
  + providing customers with technical assistance, and
  + product maintenance.

➔ **INFORMATION REQUIRED BY MARKETING SYSTEM**

1. **Environmental Information**
   - **a.** Political and governmental considerations: Information regarding political stability and government policies.
   - **b.** Demographic and social trends: Information about demography, its composition and location.
   - **c.** Economic trends: Information relating to GNP, disposable income, wage levels, productivity etc.
2. **Competitive Information**
   - **+** Information relating to business operations of competitors is extremely important in marketing management.
3. **Internal Information**
   - + Information from internal sources is more important because it affects the planning decisions at various levels of the organization. The main internal information sources are:
     1. Sales forecast
     2. Financial plan
     3. Supply factors, and
     4. Policies
   - + Information required for planning is different from information required for controlling as the former places more emphasis on structuring the future while the latter is based on immediate past and specific trends.
   - + The information required for control in marketing concerns with progress of sales plan, quotes, territories, pricing etc.

3. PRODUCTION SYSTEM

➔ Production/Operational management is one of the major areas in any kind of enterprise.
➔ It refers to those activities that are necessary to produce and deliver a service as well as a physical product.
➔ It includes purchase, warehousing, production etc.
➔ Production decisions are aimed towards:
  1. Monitoring of in process inventory,
  2. Balancing of daily finished and semi finished stocks, and
  3. Correction of any deviations in production performance.
➔ The **ROLE** of production in organizations is to provide a product that the market demands by:
  1. Producing the quantity of products needed by the customers.
  2. maintaining the quality as established, and
  3. Confirming to cost constraints imposed by production control system

➔ COMPONENTS OF PRODUCTION SYSTEM

1. Production Planning

- It means determining **what** should be produced, **when** it should be produced and **how** it should be produced.
- A **product plan** should specify:

COMPONENTS OF PRODUCT PLAN	**(a)**	the number of units of products to be produced in a given period,
	(b)	the mix of styles, sizes, colors etc of products to be manufactured,
	(c)	complete material/parts requirements through a "Bill of Material"
	(d)	labour requirement and labour operations required through a "Routing Sheet"
	(e)	Standards regarding labour operations, material and time consumption.

2. Production Control

- It includes the control of all activities related to expediting, coordinating and controlling the operations of the various production dept: or shops.
- Examples: Cost control, Time management, Quality control
- An important aspect of control is ensuring that deadlines are met.

3. **Production Scheduling**
   - It means planning the specific time at which product items should be manufactured.
   - **Objectives**
     1. To determine stages of production in sequential or rational order,
     2. To minimize idle time,
     3. To assess subcontracting needs,
     4. To ensure that production plans are met fully, and
     5. To study alternate methods of performing activities in a more effective manner.

4. **Material Requirement Planning (MRP)**
   - It has been observed that major cause of production inefficiency is lack of integrated production on planning, production scheduling and production control information systems.
   - MRP is one approach to improve production efficiency.
   - MRP integrates several production related information systems so that it can access and extract data from these systems to accomplish production scheduling.
   - **Benefits Of MRP**
     1. Reduction in both inventory levels and inventory carrying costs.
     2. Fewer stock shortages resulting in lower production interruptions.
     3. Increased efficiency of production supervisors and lesser production chaos.
     4. Better customer service by meeting deliver schedules.
     5. Greater responsiveness to change.
     6. Co ordination with marketing, engineering and finance activities.

4. COMPONENTS OF PRODUCTION SYSTEM

➔ It deals with the flow of information about people working in the organization as well as future personnel needs.

➔ Generally PIS in concerned with **6** basic subsystems of personnel function:-

1. **Recruitment:** It involves forecasting –
   - **a.** Personnel needs and skills required for recruiting people at proper time to meet manpower needs ,
   - **b.** Maintaining inventory of skills available in house.
2. **Placement:** It's concerned with matching the available persons with the requirements using behavioral tools and techniques.

3. **Training and Development :** Its concerned with keeping the workplace at par with recent technological changes and developments.
4. **Compensation :**Concerned with task of determining pay and other benefits for the workers of the concern.
5. **Maintenance :** Ensure that personnel policies and procedures are achieved.
6. **Health and Safety**

**

CHAPTER 5

DECISION SUPPORT AND EXECUTIVE INFORMATION SYSTEM

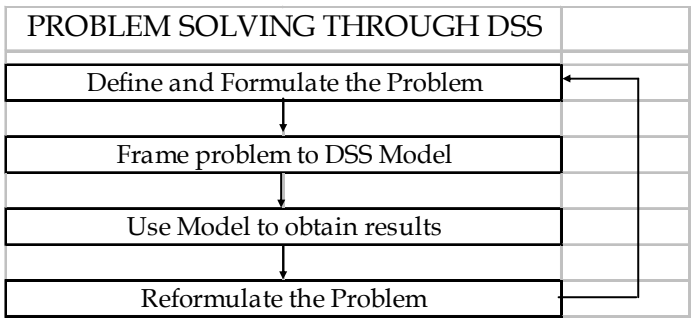
DECISION SUPPORT SYSTEMS

- ➔ Decision support systems can be defined as a system that provides tools to managers to assist them in solving semi structured and unstructured problems in their own somewhat personalized way.
- ➔ A DSS is not intended to make decisions for managers but rather to provide managers with a set of capabilities that enables them to generate information required by them in making decisions.
- ➔ DSS supports the human decision making process rather than providing a means to replace it.
- ➔ **Programmed Decision System |** These are systems used to make routine, structured decision and are intended to replace human decision making. **E.g.** Selecting audit samples, approving credit etc.
- ➔ In DSS the focus is on helping decision makers while in Programmed Decision Systems the focus is on doing something more efficiently.

DECISION SUPPORT SYSTEMS: GOALS AND APPLICATIONS

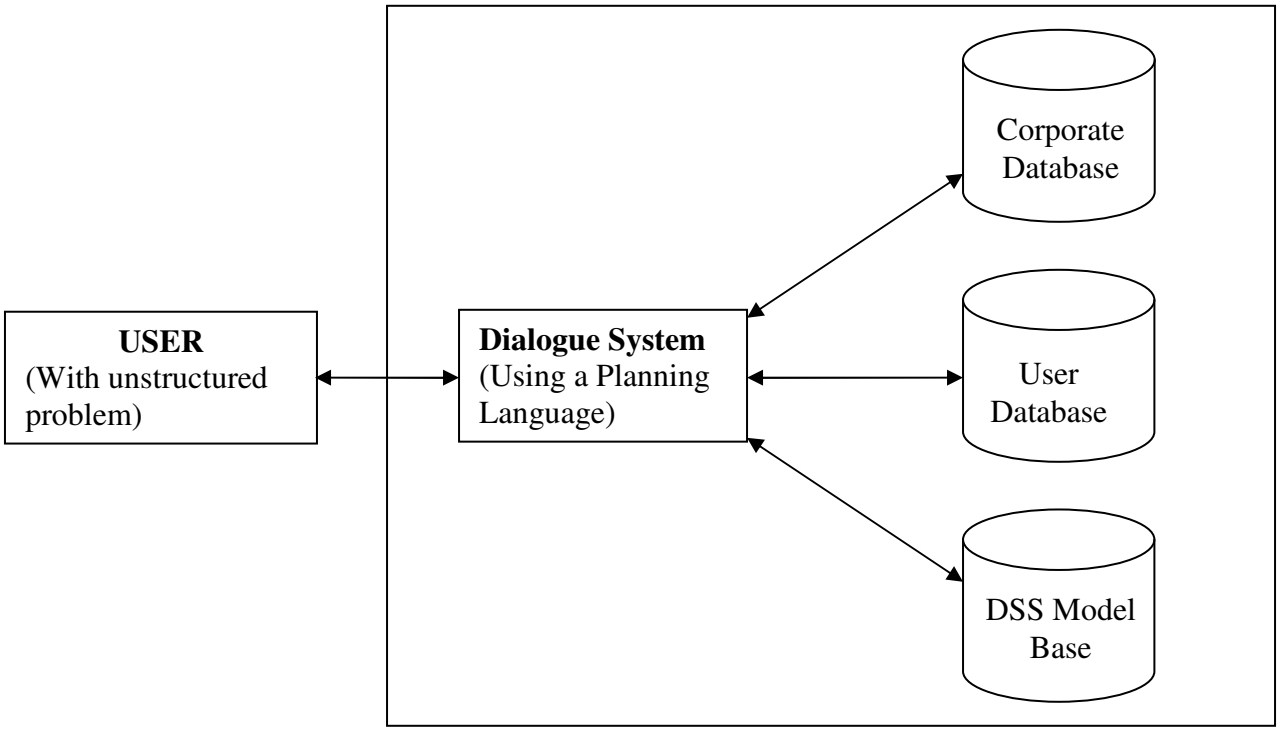
CHARACTERISTICS OF DSS

1. **They support semi-structured and unstructured decisions.**
   - + Structured decisions are those decisions that are easily made from a given set of inputs.
   - + Semi structured and unstructured decisions are however decisions for which information obtained from a computer system is only a portion of total knowledge needed to make the decision.
   - + The DSS is well adapted to help with semis structured and unstructured decisions.



2. **They are flexible enough to adapt to changing needs of decision makers.**
   - + Semi structured and unstructured decisions often do not conform to a pre defined set of decision making rules.
   - + DSS should be flexible enough to enable users to model their own information needs.
   - + DSS designer should understand that managers usually do not know in advance what information they need and the information needs keep changing.
   - + So flexibility in DSS is of paramount importance as information requests made to a DSS will often be unsystematic and distinctive.
   - + The user might request information in a variety of formats. In a well designed DSS, managers ask spontaneous questions and receive almost immediate responses for these questions.
3. **Ease of learning and use.**
   - + Since DSS is operated generally by users (managers) than computer professionals, it should be relatively easy to use.
   - + DSS tools employ user oriented interfaces non procedural Fourth Gen languages, natural English and easily read documentation.
   - + Display devices are not considered a requirement for DSS. However they are used in many DSSs.

COMPONENTS OF DECISION SUPPORT SYSTEMS



1. The User
2. Databases
3. A Planning Language, and
4. The Model Base

1. The User

+ The user of a DSS is generally a Manager with a problem to solve. The manager may at any level of authority in the organization.

2. Databases

+ DSS include one or more databases.
+ They contain both routine and non routine data from both internal and external sources.
+ DSS may construct additional databases themselves combining data from both internal and external sources.

3. Planning Language

+ There are 2 types of planning languages:
  - **(a)** General purpose Programming Languages
    These allow users to users to perform routine tasks. These languages allow users to tackle a broad range of budgeting, forecasting and other problems.
  - **(b)** Special Purpose Programming Languages
    These are often limited in what they can do but usually do certain jobs better than general purpose programming languages. E.g. Minitab
+ The planning language in a DSS allows users to maintain a dialogue with a model base.

4. Model base

+ Model base is the brain of the DSS, because it performs data manipulations and computations with data provided to it by the user and Database.
+ There are many types of Model Bases, but most of them are custom developed models that do some types of mathematical functions.
+ The analysis provided by the routines in the MIS is the key to supporting the user's decision.

TOOLS OF DSS

The tools of decision support include a variety of software supporting database query, modeling, data analysis and display.

1. **Data Base Languages**
   Tools supporting database query and report generation use mainframe, minicomputer and micro computer based databases. E.g. Dbase, Focus.
2. **Model Based Software**
   Model based analysis tools such as Spread sheet enable managers to design models that incorporate business rules and assumptions. They support model building and "What if?" types of analysis.
3. **Tools for Statistical Analysis**
   Statistical analysis software such as SAS supports market researchers, operations research analysis and other professionals using statistical analysis functions.
4. **Display based Software**
   These are used to generate graphic displays of output generated from other software, in the form of charts etc. these are very effective in management presentations.

INTEGRATED TOOLKIT

- Integrated tools provide the ability to generate, manipulate and statistically analyze data within a single software package.
- An integrated tool can transfer data from a model based software to display software or from a database to a statistics program or vice versa.

EXAMPLES OF DSS IN ACCOUNTING

- ✓ Cost Accounting System
- ✓ Capital budgeting System
- ✓ Budget variance Analysis System
- ✓ General DSS

  Some planning languages used in DSS are general purpose and therefore have the ability to analyze many different types of problems. The user needs to input data and answer questions about a specific problem domain to make use of this type of DSS. An example is program called 'Expert choice'.

EXECUTIVE INFORMATION SYSTEMS (EIS)

An EIS or Executive Support System is a DSS that is designed to meet the special needs of top level managers. ESSs are likely to incorporate additional capabilities such as E-Mail.

EXECUTIVES: An executive can probably best be described as a manager at or near the top of the organizational hierarchy who exerts a strong influence on the course taken by the organization.

EXECUTIVE ROLES AND DECISION MAKING

Most executive decisions fall into one of 3 classes:

1. Strategic Planning
2. Tactical Planning, and
3. Fire Fighting Activities

1. **Strategic Planning:** This involves determining the general long term direction of the organization.
2. **Tactical Planning:** It refers to how, when, where and what issues involved with carrying out the strategic plan.
3. **Fire Fighting:** Major problems arise sometimes that must be resolved by someone at the executive level. Many of these events will call for key alterations in plans.

CONTROL: Executive management in addition to 3 activities mentioned above also needs to exert some control over the organization. Executives will also periodically review key performance data to see how they compare against planned amounts.

THE EXECUTIVE DECISION MAKING ENVIRONMENT

The main sources of executive information are:

1. Environmental Information
2. Competitive Information
3. Internal Information

The type of decisions that executives make is broad. To a large extent executives rely much more on their own intuition than on the sophisticated analytical skills.

Five characteristics of the types of information used in executive decision making are:

1. **Lack of Structure**

   Many of the decisions executives make are relatively unstructured. It is not always obvious which data are required or how to weigh available data when reaching a decision.

2. **High Degree of Uncertainty**
   Executives work in a decision space:
   (a) that is often characterized by a lack of precedent, and
   (b) where results are not scientifically predictable from actions.
   E.g. effect of change in price on demand.
3. **Future orientation**
   Strategic planning decisions are made in order to shape future events. It's the responsibility of the executive to make sure that the organization keeps pointed towards the future.
4. **Informal Source**
   Executives rely more on informal sources for key information. These sources include meetings, chat with employees, media etc.
5. **Low level of detail**
   Important executive decisions are taken by observing broad trends which requires the executive to be more aware of large overview than tiny items.

EXECUTIVE INFORMATION SYSTEMS

An EIS is a tool that provides direct online access to relevant information in a useful and navigable format. Relevant information is timely, accurate and actionable information about aspects f business that are of particular interest to the senior manager. EIS generally designed for ease of use.

EIS VS TRADITIONAL INFORMATION SYSTEMS

- ➔ EIS is specifically tailored to executive's information needs.
- ➔ Access to data about specific issues as well as aggregate reports.
- ➔ Provide extensive online analysis tools.
- ➔ Access to broad range of internal and external data.
- ➔ Ease of use.
- ➔ Used directly by executives.
- ➔ Screen based.
- ➔ Information presented by pictorial or graphical basis.
- ➔ Information is presented in summary format
- ➔ Ability to manipulate data.
- ➔ Require large amounts of capacity and processing power within both system and the network.
- ➔ Externally focused, strategically based system.

PURPOSES OF EIS

1. To support managerial learning about an organization, its work processes and its interaction with the external environment.
2. To allow timely access to information.
3. To direct management attention to specific areas of the organization or specific business problems.

CONTENTS OF EIS

EIS implementations begin with just a few measures that are clearly of interest to senior managers and then expand in response to questions asked by those managers as they use the system.

Principles

Following is a practical set of principles to guide the design of measures and indicators to be included in an EIS:

1. EIS measures must be easy to understand and collect and if possible should be collected naturally as part of the work process.
2. EIS measures must be based on a balanced view of the organization's objectives. Data in the system should reflect organization's objectives.
3. Performance indicators in EIS must reflect every ones contribution in a fair and consistent manner.
4. EIS must encourage management and staff to share ownership of the organization's objective.
5. EIS information must be available to everyone in the organization.
6. EIS measures must evolve to meet changing needs of the organization.

**

CHAPTER 6

ENABLING TECHNOLOGIES

THE TRADITIONAL COMPUTING MODEL

1. Mainframe Architecture

In this setup all intelligence is within the central host computer (processor). Users interact with the host through the dump terminal that sends information to the host. Centralized host based computing models allow many users to share a single computer's applications, databases and peripherals.

Main *Limitations* of this kind of setup are it does not support:

a. Graphical user interfaces, and
b. Access to multiple databases from geographically dispersed sites.

2. Personal Computers

PCs made independent computing common. Independent computing models allow processing loads to be removed from a central computer. One major *Limitation* of this model is that mainframe users can't share expensive hardware peripherals and application software.

3. File Sharing Architecture

Original PC networks were based on file sharing architectures where server downloads files from the shared location to the desktop environment. The requested user job is then run in the desktop environment. However two main *Limitations* limit a file server for multi user applications.

a. It doses not support data concurrence i.e. simultaneous access to a single data set by multiple user)
b. It cannot handle multiple requests from several workstations as it flood the network.

CLIENT SERVER MODEL

Here the processing work is intelligently divided between the server and the workstation. In C/S architecture the hardware and software components (clients and servers) are distributed across a network. It's a versatile, message based and modular infrastructure that is intended to improve usability, flexibility, interoperability and scalability as compared to centralized mainframe, time sharing computing. Thus it's a form of shared or distributed computing in which tasks and computing power are split between servers and clients.

The server handles all the global tasks while the workstation handles all the local tasks. The server only sends those records to the workstation that are needed to satisfy the information request. The result of this system is that is fast, secure, reliable, efficient, inexpensive and easy to use. Server store and process data common to users across the enterprise, these data can then be accessed by client system. C/S technology facilitates provision of information that is required by a user which is easily accessed despite the physical location of the data within the organization.

Implementation examples of C/S Technology

1. Online baking application
2. Internet applications
3. E commerce online shopping page etc

BENEFITS OF C/S TECHNOLOGY

1. Improves the flow of management information.
2. Better service to end user depts.
3. Lowering IT costs
4. The ability to manage IT costs better
5. Direct access to required data
6. High flexibility of information processing
7. Direct control of the OS
8. Increased productivity.
9. Takes less people to maintain a C/S application than mainframe based applications.
10. Easiness in implementing C/S when compared to a legacy application.

CHARACTERISTICS OF C/S TECHNOLOGY

1. Client server architecture consists of a client process and a server process that can be distinguished from each other.
2. Client and Server can operate on separate computer platforms.
3. Either the client platform or the server can be upgraded without having to upgrade the other.
4. Server can service multiple clients concurrently.
5. C/S system includes some kind of networking capability.
6. A significant portion of the application portion logic resides at the client end.
7. Action is usually initiated at the client end.
8. GUI at client end
9. SQL capability
10. The database server should provide data protection and security.

APPROACHES TO CLIENT/SERVER

- C/S computing is based on the fact that programmable desktop computer can be used to do most of the application processing.
- C/S computing allows applications to be broken down to many different jobs and each task can be run on a different platform, under a different OS with different network protocols.
- Each task can be maintained and developed separately which in turn accelerates application development.
- Applications can be divided into 6 tasks :
    1. User interface,
    2. Presentation logic,
    3. Application logic,
    4. Data requests and Result acceptance
    5. Data integrity, and
    6. Physical data management
- **Elements of C/S Computing process**
    1. Data storage: allows retrieval of data
    2. Database management system: organize the data
    3. Application software: provides integration of storage and DBMS
    4. OS: control and allocate resources of the computing system
    5. User interface (UI): allows end user to communicate with program.
    6. Display devices: allows the user to monitor and communicate with UI.

COMPONENTS OF CLIENT SERVER ARCHITECTURE

1. Client

- A client is "any system or process that can request and make use of data, services or access to other systems provided by a server"
- Client is typically a PC.
- **Types of Clients**
    1. Non GUI Clients: require minimum amount of human interaction. E.g. ATM
    2. GUI Clients: these are human interaction models.
    3. Object oriented UI Clients: facilitates object interaction rather than application interaction

2. Server

- A server is "any system or process that provides data, services or access to other systems for clients most often for multiple clients simultaneously".
- **Types of Servers**
  1. File Servers: make it possible to share files by maintaining a share library of docs.
  2. Database servers: enables SQL queries.
  3. Transaction servers: used to execute a series of SQL commands
  4. Web servers: allows clients and servers to communicate with HTTP protocol.

3. Middleware

- It's the network system implemented within the client /server technology. It includes all the distributed software needed to allow clients and servers to interact.
- **Layers of Middleware**
  1. Service: carries coded instructions and data from applications to next layer.
  2. Back end processing: encapsulates network routing instructions in such data.
  3. Network OS: adds additional instruction to ensure data is sent to correct user.
  4. Transport stacks: transport data packets to designated user efficiently.

4. Fat Client or Fat Server

- In a Fat-client system more of the processing takes place on the client, and
- In a Fat-server system processing takes place in the server and try to minimize the processing by clients.

5. Network

- It involves both the network hardware like cabling, cords etc and network software used to manage traffic over the network.

CLIENT SERVER SECURITY

To get secured client/server environment all access points should be known. An IS auditor should ensure that the following control techniques are in place to increase the security.

- Access to data and application is secured by disabling the floppy drive.
- Diskless workstation prevents unauthorized access.
- Unauthorized users may be prevented from overriding login scripts and access by securing automatic boot or startup batch files.
- Network monitoring utilities can be used to monitor the clients.
- Data encryption techniques are used to protect data from unauthorized access.
- Authentication system that requires a login name and password can be provided to clients to restrict access.
- Smart cards that display a temporary password based on an algorithm can also be used.
- Application controls can be used to restrict access within the application.

CLIENT / SERVER RISKS AND ISSUES

There are four main categories of risks involved in the transition from mainframe to Client/Server system.

1. **Technological Risks**
   There is a risk that in the long run the system may grow obsolete. That it will become obsolete is probably inevitable thus the question becomes- how soon it will become obsolete.

2. **Operational Risks**
   These risks run parallel to technological risks and include:
   (a) the risk of under performance
   (b) the risk that the software may not flexible enough to adapt to changing needs of the organization.

3. **Economic Risks**
   In the short run costs will increase as the firm has to maintain both the mainframe system and client/server system. In the long run maintenance costs may result in high costs.

4. **Political Risks**
   In the short run there is a risk that the employees may reject the new system if the system is difficult to use.

SERVER - CENTRIC MODEL

- **Total Cost of Ownership :** TCO considers 2 types of costs-
  1. Acquisition costs: This represents substantial one time investments.
  2. Recurring or Soft Costs
- Server centric computing is a model, in which applications are deployed, managed supported and executed 100% on a server. The client handles the data entry and information display.
- It uses multi user OS and a method for distributing the presentation of an applications interface
- With server based computing, client devices have instant access to business critical applications via the server.
- Server based computing can work within the current computing infrastructure and current computing standards.
- In a server based system the overall performance is primarily depended upon network bandwidth and the number of users connecting simultaneously.
- **Benefits**
  1. It enables the organization to bring Heterogeneous computing environments.
  2. It offer enterprise scale management tools to allow IT professionals to scale, deploy, manage and support applications from a single location.
  3. It provides seamless desktop integration of the user's local and remote resources.

**

CHAPTER 7

SYSTEM DEVELOPMENT PROCESS

SYSTEMS DEVELOPEMNT PROCESS

- ➔ Systems development refers to the process of examining a business situation with the intent of improving it through better procedures and methods
- ➔ Its has 2 major **components:**

1. **Systems Design:** This is the process of planning a new business system or one to replace or complement an existing system.
2. **Systems Analysis**: This is the process of :
   - **i.** gathering and interpreting facts,
   - **ii.** diagnosing problems, and
   - **iii.** Using the information to recommend improvements to the system (solve the problems)**.**

   System analysts assess what the future need of the system will be and what changes should be considered to meet these needs. They recommend alternatives for improving the system.

   A plan which includes all system design features, file specifications, operating procedures design features and equipment and personnel requirements is developed.

SYSTEM DEVELOPMENT LIFE CYCLE

The system development life cycle can be thought of as a set of activities that analysts, designers and users carry out to develop and implement an information system. It starts with identification of the need to improve existing system. It involves **6 activities** which are closely related.
The system development life cycle method **consists of following activities**:

1. **Preliminary Investigation**
   - A preliminary investigation is undertaken when users come across a problem or opportunity and submit a formal request for a new system to the MIS Dept
   - This involves **Three** parts:
     1. Request clarification (to determine what the originator really wants)
     2. Feasibility Study (technical, operational and economic feasibility)
     3. Request approval

2. **Requirements analysis (Systems Analysis)**
    - Analysts work closely with employees and mangers of the organization for determining information requirements of the users.
    - Several fact finding tools like interviews etc are used to understand the requirements.
    - As details are gathered the analysts study the present system to identify its problems and shortcomings and identify the features, which the new system should include to satisfy the new or changed user application environment.

3. **Design of System**
    - The user requirements that arose in the System analysis stage are incorporated into a new systems design.
    - The design of an information system produces the detail that state how a system will meet the requirements identified in analysis stage.
    - The analysts design various reports, databases etc and these design specifications are then passed on to the programming staff.

4. **Acquisition and Development of Software**
    - After completion of systems design the resources' needs (hardware, software and services) are determined. Choices are made regarding which products to buy or lease from which vendors.
    - The software required may either be purchased or developed in house.

5. **Systems Testing**
    - Testing is done experimentally to ensure that software does not fail i.e. it will run according to its specifications and in the way users expect.

6. **Implementation and maintenance**
    - After the system is found to be fit, its implemented with actual data. Hardware and software are installed and people are trained to work in the new system.
    - After implementation the system is maintained i.e. its modified to adapt to changing needs and users so that to increase the productive life of the system.

The system development life cycle is a continuous iterative process that recycles through each stage for many applications. Even when a system is fully specified, designed, purchased and running, it's continually being enhanced or maintained.

REASONS FOR FAILURE TO ACHIEVE SYSTEMS DEVELOPMENT OBJECTIVES

1. Lack of senior management support for and involvement in information system development.
2. Shifting user needs.
3. Development of strategic systems (since strategic decision making is unstructured the requirements and specifications for such development projects are difficult to define).
4. New technologies (personnel may not be familiar with latest technology).
5. Lack of standard project management and systems development methodologies.
6. Overworked or under-trained development staff.
7. Resistance to change.
8. Lack of user participation.
9. Inadequate testing and user training.

APPROACHES TO SYSTEMS DEVELOPMENT

1. TRADITIONAL APPROACH

- In the traditional approach of the systems development activities are performed in sequence, beginning with preliminary investigation and ending in system implementation and maintenance.
- Managers and users are most likely to interact with systems analytics, systems designer and application programmers when the traditional approach is used.
- Under traditional approach an activity is undertaken only when the prior step is fully completed. Managers and users consider and review the work performed by MIS professionals during each stage of process before proceeding to the next stage.
- This approach is applied to the development of larger computer based information systems such as the transaction processing systems. Because the processing requirements of these systems are well understood, the risk of users and systems analysts misperceiving the system are less.

2. PROTOTYPING APPROACH

- Since the development time in traditional approach is more, it is not suitable to develop smaller systems such as DSS, MIS and Expert systems. To develop such environments, prototyping approach is used.
- The goal is to develop a small or pilot version called 'prototype' of part or all of the system.

- A prototype is a usable system or system component that is built quickly and at a lesser cost, and with the intention of being modifying or replacing it by a full scale and fully operational system.
- As users work on the prototype they make suggestions as to its weak points. These suggestions are used to design and develop the real system.
- Prototyping helps users to identify additional requirements and needs. Hence this approach can be used to develop systems which require continuous refinements like expert systems.
- **Steps In Prototyping**
    1. Identify information system requirements
    2. Develop the initial prototype (Rapid development and low cost)
    3. Test and Revise (this process continues till users are satisfied)
    4. Obtain user sign off of the approved prototype (final approval by users)
- **Conditions for adopting Prototyping**
    1. End users don't understand their informational needs very well,
    2. System requirements are hard to define
    3. The new system is mission critical or is needed quickly
    4. Past interactions have resulted in misunderstandings between end users and designers
    5. The risks associated with developing and implementing the wrong system is high.
- **Advantages**
    1. Requires intensive involvement of users and this result in a better system.
    2. A prototype can be developed within a short timeframe and immediately it can be evaluated by users.
    3. Continuous development helps to design a bug free system as most of the bugs in the prototype would have been detected by the users and eliminated. Hence the final system will be more reliable.
- **Disadvantages**
    1. Users may not be willing or able to devote the amount of time required under this approach.
    2. Since under this approach prototypes are tested extensively, developers are frequently tempted to minimize the testing and documentation process of the final system. This makes the final system error prone and hard to maintain.
    3. Users have to go through a number of interactions with prototypes. This may cause behavioral problems with system users (dissatisfaction)
    4. Design team can be mislead if it relies on a small portion of the user population for developing its models. Hence it cannot be used to develop large or complex systems.

3. END USER DEVELOPMENT APPROACH

- In this approach the end users are responsible (and not the computer professionals) for systems development activities. Availability of low cost technology has made this approach more feasible in recent times.
- **Risks in adopting End User development Approach**
    1. A decline in standards and controls *as standards etc may not be as rigorously enforced by the end user.*
    2. Inaccuracy of specification requirements. *The end user will not have the experience of an analyst in completing the accurate specification of system requirements.*
    3. Reduction in the quality assurance and stability of the system.
    4. An increase in unrelated and incompatible systems.
    5. Difficulties in accessing central database *with proliferation of different systems and applications.*

4. TOP DOWN APPROACH

- As per this approach the organization's goals should be the driving force behind development of all computer systems. Hence the information system should be responsive to and supportive of an organization's objectives.
- Top down approach assumes a high degree of top management involvement in the planning process and focuses on organizational goals, objectives and strategies.
- **Stages in Top down Approach**
    1. Analyze the objectives and goals of the organization to determine where it is going and what top management wants to accomplish. It's also determined what resources are available in terms of capital, equipment and raw materials.
    2. Identify the functions of the organization and explain how they support the organization.
    3. Ascertain the major activities, decisions and functions of the managers at various levels of hierarchy.
    4. Identify models that guide managerial decision making process and find out the information requirements for activities and decisions.
    5. Prepare specific information processing programs in detail and modules within these programs.

5. BOTTOM UP APPROACH

- The development of information systems under this approach starts with the identification of "Life Stream Systems" (those systems which are essential for day to day business activities), e.g. Payroll. For each such life stream system an Information system is developed.
- **Steps**
  1. Identifying their
     i. Basic transactions,
     ii. Information file requirements and
     iii. Information processing programs.
  2. Development of Information system for each life stream system
  3. Integration of data kept in different data files of each information system. This enhances the share ability and evolvability of the database.
  4. Addition of decision models and various planning models for supporting the planning activities involved in management control. These models are integrated to evolve model base.

Comparison of Top Down and Bottom up Approaches

Sl	Area	Top Down Approach	Bottom Up Approach
1	Formulation of major objectives and strategies.	Top management takes the initiative.	Supervisory management.
2	Development of System	By Top management. Middle and Supervisory managers have little role.	By Middle and Supervisory levels of management.
3	Integration	Information system fully integrated	Information system may not be fully integrated.

6. SYSTAMATIC APPROACH

- This approach is adopted in smaller organizations.
- **Steps**
  a. Identify requirements.
  b. Locate, evaluate and secure suitable software.
  c. Locate, evaluate and select suitable hardware.
  d. Implement the system.

PROJECT MANAGEMENT

➔ Recent surveys have showed that poor project management played a significant role in IT project failures and pointed out following as the main reasons for failed systems.

➔ **Reasons for Failure**

1. Underestimation of the time to complete the project.
2. lack of control by senior management
3. underestimation of required resources
4. inadequate planning
5. inadequate project control mechanism

➔ **Elements of Project Management.**

1. User participation in defining and authorizing the system
2. Assignment of appropriate staff to the system development and definition of their authorities and responsibilities.
3. A clear written statement of system nature and scope.
4. A feasibility study
5. A system master plan
6. A risk management program
7. Division of the system to manageable processes
8. Approval of work accomplished in one phase before working on the next
9. Integration of the quality assurance plan with system master plan

SYSTEM DEVELOPEMNT (LIFE CYCLE) METHADOLOGY [SDLC]

➔ SDLC is a formalized, standardized, documented set of activities used to manage systems development project. It should be used when information systems are developed, acquired or maintained.

➔ **Characteristics of SDLC Methodology**

1. A project is divided into a number of identifiable processes. Such division facilitates both project planning and project control.
2. Specific reports and other documentation (Deliverables) are produced periodically during system development to make personnel accountable for faithful execution of system development tasks.
3. Users, managers and auditors are required to participate in the project.
4. System is tested thoroughly prior to implementation

5. A training plan is developed for those who will operate and use the system
6. Formal program change controls are established to preclude unauthorized changes
7. A post implementation review to assess effectiveness and efficiency of the new system.

➔ **Systems Development Standards Manual**: An organization's SD methodology should be documented in the form of a *Systems Development Standards Manual.* It should indicate:
- ☞ Methods for requesting systems development
- ☞ Procedures to be followed, techniques to be used and documentation to be prepared during systems development.
- ☞ Reviews to be performed and signoffs to be obtained.

➔ **Systems Development Team:** Several people in the organization are responsible for systems development.
- Usually in big organizations the worth of a particular project and progress of an ongoing project is assessed by top management and a steering committee consisting of top IS services users.
- IS Dept is responsible for the development of the system. A project management team consisting of computer professionals and key users is formed to coordinate the development activities.
- System users and end users also play a key role in the design and development of an IS.

➔ **Accountants Role in Development Activities:**
- Accountants are uniquely qualified to participate in systems development as they can combine knowledge of IT, Business, accounting and internal control as well as behavior and communication.
- Accountants provide a unique and independent perspective with which to evaluate the systems development process and the systems being developed.

SYSTEM DEVELOPMENT LIFE CYCLE : IN DETAIL

1. PRELIMINARY INVESTIGATION

➔ System development starts with identification of a problem by the management or users.

➔ Shifting business requirements, changing organizational requirements and evolving information technology may render existing systems ineffective or inefficient or may call for a new system.

➔ To consider changing the system, planned reviews are conducted to determine whether:

1. The System Still Satisfies Users' Information Needs,
2. New Design Ideas Can Be Incorporated To Existing Structure
3. Evolving Environmental Changes Require System Changes
4. New Business Ventures By The Entity Requires Change In System
5. User Requests A Change

➔ If the need seems genuine, a System Analyst is assigned by the steering committee to make a preliminary investigation to identify those projects which are most beneficial to the organization.

➔ Preliminary investigation relates to collection of information that permits committee members to evaluate the merits of the project request and make an informed judgment about the *feasibility* of the proposed project. Its neither a designed study nor it includes collection of details to completely describe the business system.

➔ **Objectives Of Preliminary Investigation**

1. Clarify and understand the project request
2. Determine the size of the project
3. Determine the technical feasibility of alternate approaches
4. Assess costs and benefits of alternate approaches
5. Report findings to the management with recommendations outlining the acceptance or rejection of the proposal

➔ **Conducting The Investigation (Collection of Information)**

1. Reviewing Internal Documents : The analysts conducting the investigation first try to learn about the organization involved in, or affected by, the project by examining organization charts and studying written operating procedures.

2. Conducting Interviews: Interviews allow analysts to know more about the nature of the project request and the reasons for submitting the request.

➔ **Identifying Viable Options:** After identifying problems or opportunities the analyst must determine-

1. the scale of response to meet the users requests for a new system, and
2. the approximate amount of time and money that will be required in the effort

The analyst then compares possible solutions to reach a final decision. Common sense and intuition are key ingredients in the solution development process.

➔ **Testing Project's Feasibility:** Feasibility study refers to a process of evaluating alternative systems through cost/benefit analysis so that the most feasible and desirable system can be selected for development. Its undertaken mainly from 3 angles:

1. Technical
2. Economic, and
3. Operational

1. **Technical Feasibility:** System Analysts ascertains whether the proposed systems is feasible with existing or expected computer hardware and software technology. Some of the technical issues raised are:
    a. Existence of necessary technology
    b. Capacity of existing equipment
    c. Expansion of the system in future
2. **Economic Feasibility:** Evaluation of all the incremental costs and benefits expected if the proposed system is implemented. Some of the issues raised are:
    a. The cost of conducting a full systems investigation
    b. The cost of hardware and software being considered
    c. The benefits (reduced cost and errors)
    d. The cost if the proposed system is not developed.
3. **Operational Feasibility:** Ascertaining the views of workers, employees, customers and suppliers about the use of computer facility. Some of the issues raised are:
    a. Support from managers and users
    b. Involvement of users in planning and development as their involvement results in lesser resistance
4. **Schedule Feasibility:** Estimating how long it will take a new or revised system to become operational and communicating this information to the steering committee.
5. **Legal Feasibility:** It's concerned with whether there will be any conflict between a newly proposed system and the organizations legal obligations.

➔ **Estimating System Costs:** System costs can be divided into 3 categories:

1. Development,
2. Operational, and
3. Intangible Costs

1. **Development Costs:** It includes costs of the system development process such as salaries of system analysts, costs for preparing system manuals and cost of preparing new or expanded computer facility.
2. **Operational Costs:** These include hardware/software rent/depreciation, salaries of computer operators, cost of input data preparation and control, cost of data processing supplies etc.
3. **Intangible Costs:** It's very difficult to measure intangible costs and includes gain/loss of employee morale, goodwill etc.

➔ **Estimation of Benefits:** The benefits which result from developing new or improved information systems that utilizes EDP can be subdivided into tangible and intangible benefits.

1. **Tangible Benefits:** These can be accurately measured and are directly related to the introduction of a new system such as decrease in data processing costs.

2. **Intangible Benefits:** These cannot be measured and include improved business image/goodwill.

Following are some of the benefits of development of a computerized system:

1. Increase in sales
2. Decrease in operating costs
3. Improved customer service through timely service
4. Improved managerial decision making
5. New or improved information availability

➔ **Reporting Results to Management:** After the analyst articulates the problem and its scope, provides one or more solution alternatives and estimates the costs and benefits of each alternative, he reports these results to management. He also makes a recommendation regarding further procedures. Management after careful evaluation of this report decide on further action.

2. REQUIREMENT ANALYSIS / SYSTEMS ANALYSIS

➔ **Under Traditional Approach:** In this stage the focus is on

1. determining user needs,
2. studying the application area in depth,
3. assessing strengths and weaknesses of the present system, and
4. reporting results to management.

➔ **Under Prototype Approach:** Here the requirement analysis and design phases proceed in tandem and in small increments.

➔ **Objectives:**

1. Determining the manner in which the system uses hardware, software and human resources to convert the data of the organization into information for end users,
2. Assessing how the resources are used to accomplish the activity f input, processing, output, storage and control.

➔ **Fact Finding Techniques:** Various fact finding techniques used to determine the needs of users are:

1. Documents: Manuals, Input/output forms, diagrams etc
2. Questionnaires
3. Interviews: Plays a larger role in prototyping
4. Observation

➔ **Analysis of the Present System:** Detailed investigation of the present system involves collecting, organizing and evaluating facts about the system and the environment in which it operates. The following areas should be studied in depth:

1. Review of historical aspects

   A brief history of the organization (Annual reports) is a logical starting point for an analysis of the existing system. A historical review of the organization chart can identify the growth of management levels as well as development of various functional areas and depts.

2. Analyze inputs

   A detailed analysis of present inputs is important since they are basic to the manipulation of data. The system analyst should be aware of the various sources from where the data are initially captured, keeping in view the fact that the outputs for one area may serve as input for another area.

3. Review data files maintained

   The analyst should investigate the data files maintained by each dept noting thir size, location etc. Information on common data files and their size will be an important factor which will influence the new information system. He should also review all on line and off line files that are maintained in the organization.

4. Review methods, procedures and data communications

   Methods and procedures transform input data into useful output. A ***method*** is a way of doing something; a ***procedure*** is a series of logical steps by which a job is accomplished. A ***procedure review*** is an intensive survey of methods by which each job is accomplished, the equipment used and the actual location of the operations. Its objective is to eliminate unnecessary tasks or to perceive improvement opportunities in the present information system.

   The system analyst must understand how the data communications network is used in the present system so as to identify the need to revamp the network when the new system is installed.

5. Analyze outputs

   The system analyst should analyze the outputs to determine how well they will meet the organization's needs. He must understand what information is needed and why, who needs it and when & where it is needed. Attempt should be made to eliminate reports that have no relevance to current operations.

6. Review internal controls

   An examination of the present system of internal controls may indicate weaknesses that should be removed in the new system.

7. Model the existing physical system and logical system.
   After each item is reviewed the process is documented. The logical flow of the present information system is depicted in the form of System Flow Charts and the physical flow is depicted using Data Flow Diagrams. Each major operation in the System Flow Chart is broken down to its lowest level modules and the data flow diagram is drawn for each.
   The flow charting helps to organize the facts and to disclose gaps and duplication in data gathered.

8. Undertake overall analysis of present system
   The final phase of the detailed investigation includes the analysis of :
   a. The present work volume
   b. The current personnel requirements, and
   c. The present benefits and costs

➔ **System Analysis of Proposed Systems:** After each functional area of the present information system is carefully analyzed, the proposed system specifications are defined based on the objectives set forth at the first stage of study and the strengths and weaknesses of the present system.
The starting point for compiling system specifications is Output as it is directly related to the objectives of the organizations. After outputs have been determined it is possible to infer what inputs, database, methods, procedures and data communication must be employed.
After completing these steps the information gathered is documented in ***the Explanatory Survey Report*** which is authorized by the team of system analysts and approved by user group. The report is then submitted to the steering committee.

SYSTEM DEVELOPMENT TOOLS

➔ **Objectives / Utility of System development tools:**

1. To conceptualize, clarify, document and communicate the activities and resources involved in the organization and its information systems.
2. To analyze present business operations, management decision making and information processing activities of the organization.
3. To propose and design new or improved information system to solve business problems or pursue business opportunities that have been identified.

➔ **Categories of System Development Tools (based on the system features each document has):**

1. System Component and Flows

   These tools help the system analysts to document the data flow among the major resources and activities of an information system. Examples:

   a. System Flow Charts
   b. Data Flow Diagram
   c. System Component matrix (provides a matrix framework to document the resources used, the activities performed and the information produced by an information system)

2. User Interface

   These tools are used to design the interface between the end users and the computer system. Layout forms and screens are used to construct the formats and contents. Dialogue Flow diagrams analyze the flow of dialogue between computers and people.

3. Data attributes and relationships

   This category of tools is used to define, catalogue and design the data resources in information system. Examples:

   a. Data dictionary: catalogues the description of the characteristics of all data elements and their relationships to each other as well as to external systems.
   b. Entity relationship diagrams: document the number and type of relationship among the entities in a system.
   c. File layout forms: document the type, size and names of the data elements in a system.
   d. Grid charts: helps in identifying the use of each type of data element in input / output or storage media of a system.

4. Detailed system process

   These tools are used to help the programmer develop detailed procedures and processes required in the design of a computer program.

   a. Decision Trees / Tables: use a network or tabular form to document the complex conditional logic involved in choosing among the information processing alternatives in a system.
   b. Structure charts: document the purpose, structure and hierarchical relationships of the modules in a program.

➔ **System development tools in detail:**

1. Systems Flow Chart

   It's a graphic diagramming tool that documents and communicates the flow of data, media and information processing procedures taking place in an information system using a variety of labeled symbols connected by arrows to show the sequence of information processing activities. These are widely used to communicate the overall structure and flows of a system to end-users.

2. Data Flow Diagrams (DFD)

   A DFD graphically describes the flow of data within an organization. It's composed of four basic elements:

   a. Data sources and destinations (Symbol: A Square) > it represents an organization or individual that sends or receives data used or produced by the system.
   b. Data flows (Symbol: An Arrow) > it represents the flow of data between processes, data stores and data sources/destinations. A data flow can consists of one or more pieces of datum. If these multiple data elements don't flow together multiple lines are drawn to depict these elements.
   c. Transformation processes (Symbol: A Circle) > these represent the transformation of data.
   d. Data stores (Symbol: Two parallel Horizontal lines) > a data store is a temporary or permanent repository of data. DFDs don't show the physical storage medium used to store data.

   These 4 symbols are used to show how data are processed.

   - Subdividing the DFD: DFDs are subdivided into successively lower levels in order to provide increasing amounts of detail.
   - Context Diagram: The highest level DFD is referred to as a context diagram. It provides a summary level view of the system depicting data processing system and external entities that are the sources and destinations of the inputs and outputs.

3. Layout Forms and Screens:

   These consist of electronic displays or preprinted forms on which the size and placement of titles, heading, data and information can be designed. these are used to design source docs, input/output and storage records, Files and output displays and reports.

4. System Component Matrix

   It views the information system as a matrix of components that highlights how basic activities of input, processing, output, storage and controls are accomplished in an

information system and how the use of hardware, software and people resources can convert data resources into information products.

5. CASE Tools

   CASE stands for Computer Aided Software Engineering. It refers to the automation of anything that humans do to develop systems. CASE tools today can support all phases of traditional system development process.

6. Data Dictionary

   A Data Dictionary is a computer file that contains descriptive information about the data items in the files of a business information system. Thus it's a computer file about data. Each record of a data dictionary contains information about a single data item used in a business information system. A Data dictionary may include:

   - Contents of a Data dictionary
     1. Codes describing the data items length, data type and range.
     2. Identity of source docs used to create the data item.
     3. Names of the computer files that stores the data item
     4. Names of the computer programs that modify the data item
     5. Identity of the computer programs or individuals permitted to access the data item.
     6. Identity of the computer programs or individuals not permitted to access the data item.
   - Uses of a Data Dictionary
     1. It's a documentation aid to programmers and system analysts.
     2. Useful for file safety as it lays down users who can and cannot access the items.
     3. It provides an audit trail as source docs can be identified.
     4. It can be used to plan the flow of transaction data through the system.
     5. It's an important aid when investigating or documenting internal control procedures.

**

CHAPTER 8
SYSTEMS DESIGN

SYSTEMS DESIGN

- The systems design phase consists of the following three activities:
    1. Reviewing the systems informational and functional requirements;
    2. Developing a model of the new system including logical and physical specifications of outputs, inputs, processing, storage, procedures and personnel; and
    3. Reporting results to management.
- The systems design must confirm to the purpose, scale and general concepts of the system that management approved during the requirement analysis phase.
- System design involves first logical and then physical construction of a system.
- In logical design phase design specifications of the systems are established.
- Physical construction produces program software, files and a working system.

DESIGNING SYSTEM OUTPUTS

- The term output applies to any information produced by an information system, whether printed or displayed.
- System output may be a report, a document or a message.
- When analysts design computer output, they
    - Identify the specific output that is needed to meet the information requirements,
    - Select methods for presenting information, and
    - Create documents, reports or other formats that contain information produced by the system.
- Without quality output the entire system may appear to be so unnecessary that users will avoid using it possibly causing it to fail.

➔ **Output Objectives**

1. Convey information about past activities, current status or projections of the future,
2. Signal important event, opportunities, problems or warnings
3. Trigger an action
4. Confirmation of an action

Good systems output design cannot be developed independent of the uses of output. It must meet the needs of the organization.

➔ **Important Factors in Output Design**

1. Content
   It refers to the actual pieces of data included among outputs provided to users. Too much content can cause managers to waste time in isolating the information that they need; it also diminishes the impact of truly important information. Hence only the required information should be included in various outputs.
2. Form
   It refers to the way the content is presented to users e.g. quantitative, text, graphics video and audio.
3. Output Volume
   The amount of data output required at any one time is known as output volume.
4. Timeliness
   It refers to when users need outputs. Some outputs are required on a regular periodic basic while others are generated on a request.
5. Media
   It refers to the physical device used for input, storage or output e.g. paper, video display etc.
6. Format
   Format is the manner in which data are physically arranged. Format of information reports should be so devised that it:
   - Assists in decision making,
   - Identifying and solving problems,
   - Planning and initiating corrective action and
   - Searching

   Codes and abbreviations must be avoided to increase clarity. Reports should be supplied on an exception basis to save the managers from information overload. It is also to be ascertained that the cost of the report is justified by the benefit.

➔ **Guidelines for Presentation of Information**

1. **Tabular Format**
   - Generally end users are most accustomed to receiving information in a tabular form.
   - Tabular format should be used when
     - Details dominate and few narrative comments are needed,
     - Details are to be presented in discrete categories.
   - Each category must be labeled and totals must be drawn or comparison made between components.

- The items that should be included in tabular outputs are:
    I. Exceptions to normal expectations,
    II. Major categories or groups of activities or entities
    III. Summaries of major categories or activities
    IV. Unique identification information
    V. Time dependent entities.

2. Graphic Format

- Business graphics makes use of various types of charts and maps e.g. pie charts, bar charts, area charts etc.
- Graphics are superior to tabular or narrative forms of information display for
    - detecting trends in business performance,
    - comparing different information
    - remembering large amounts of data
- **Standards in designing graphics**
    - Graphical outputs should be designed keeping in mind
        - The purpose of the graph
        - The kind of data that need to be displayed
        - Its audience, and
        - The effects on the audience of different kinds of graphical output.
    - It should include a title and date of preparation. For a series page numbers should also be included.
    - Labels and common type styles should be inserted so as to increase readability.
    - As far as possible abbreviations should not be used
    - Users must be trained to interpret the output.

➔ **Designing Printed Output**

- An output layout is the arrangement of items on the output medium.
- The layout should show
    - The location and position of all variable information such as item details, summaries and totals, control breaks and
    - All preprinted details such as headings and titles.
- The layout is a blue print that will guide the construction of programs later in the development process.
- **Guidelines for Preparing the layout form**
    1. Reports should be designed to read from left to right and top to bottom
    2. The most important items should be easier to find.

3. Report should include a short and descriptive heading, date of preparation, column headings and page numbers.
4. Each data item must have a short and descriptive heading.
5. Control breaks, separated from the rest of the data with additional lines, should be used to increase readability.
6. Sufficient margin should be left on the right, left, top and bottom of the report.
7. The detail line for variable data should be defined.
8. The mockup of reports should be reviewed for feasibility, usefulness, readability, understandability and an aesthetic appeal.

➔ **Designing Visual Display Output**

- Many of the principles of good design for printed output also apply to output shown on VDUs.
- **Factors to be considered before designing Visual Display Output**
    1. Physical dimensions of the screen
    2. Number of rows and columns of data that can be displayed
    3. Degree of resolution
    4. Color depth
    5. Methods of highlighting (bold, italics etc)
    6. Methods of intensity controls
- It's helpful to divide the display screen to sections that are consistently used in the same way to present information, identifications and messages to the user.
- In designing output screens the user may need areas for:
    a. Headings and titles
    b. Content
    c. Messages and instructions
    d. Explanations (help)

➔ **Designing Windows**

- Windows are sub divisions of the display screen that makes it possible to present different sets of output simultaneously.
- **User requirements / Windowing Capability**
    - Ability to reposition the windows on the display screen
    - Ability to resize the windows
    - Capability to hide unused windows
    - Overlapping (it allows users to move information the foreground when its needed and to replace it again with other information)

- **Uses / Advantages of Using Windows**
    a. Display different sets of data or report sets simultaneously,
    b. Switch between several programs / outputs,
    c. Move information from one window to another of the same program, and
    d. Permits users to reposition of windows according to their needs.

DESIGNING SYSTEM INPUTS

- Input design consists of
    - Developing specifications and procedures for data preparation,
    - Developing steps which are necessary to put transactions data into usable form for processing, and
    - Data entry.
- Starting point for the input design process is a review of the information compiled during the requirement analysis phase. The review highlights basic problems and difficulties with the present system.

➔ **The input issues to consider for design of input specifications**

1. Content
   The analyst is required to consider the types of data that are needed to be gathered to generate the desired user outputs
2. Timeliness
   It's important that the data is inputted to computer in time because outputs cannot be produced until certain inputs are available.
3. Media
   It refers to the choice of input media and subsequently the devices on which to enter data e.g. display workstations, magnetic tapes etc
4. Format
   It refers to defining the type and length of each data filed and other special characteristics.
5. Input volume
   It refers to the amount of data that has to be entered in the computer system at any one time.

➔ **Capturing Data for Input**

- The quality of input determines the quality of system output.
- Well defined input forms and visual display terminal screens should meet the **objectives** of
    - effectiveness,
    - accuracy,
    - ease of use,

- consistency,
- simplicity and
- attractiveness

➔ **Form Design**

- Forms are pre printed papers that require people to fill in responses in a standardized way
- **Guidelines in Form Design**

  The following are some guidelines for form design:

  1. Easy to fill forms

     The forms should generally be easy to fill out. This can be achieved by considering the following factors:

     a) *Form Flow* – form should flow from left to right and top to bottom
     b) *Divide forms in logical sections* – A good form consists of following 7 main sections:
        - Headings
        - Identification and access
        - Instructions
        - Body
        - Signature and verification
        - Totals, and
        - Comments
     c) *Captioning* – Captions tell the persons completing the forms what to put on a blank space.

  2. Meeting the intended purpose

     Forms are created to serve one or more purposes in the
        - Recording,
        - Processing,
        - Storing, and
        - Retrieving of information of various businesses.

  3. Ensuring accurate completion

     Internal double checks can be inserted into a form to ensure the accuracy of data filled in by the user. E.g. checking column and row totals.

  4. Keeping forms attractive

     An aesthetic form draws people into it and encourages proper completion. Forms should look uncluttered, organized and logical even after they are filled in. Type fonts and line weights are useful design elements for capturing attention and forcing people to fill the form correctly.

➔ **Coding Methods**

- Coding methods in which conditions, words or relationships are expressed by a code to reduce input, control errors and to speed up the process.
- A **code** is a brief number, title or symbol used instead of lengthy or ambiguous description.
- With code, fewer details are necessary in input but it results in no loss of information.
- The system analyst is responsible for devising an appropriate coding sceheme.
- **Desired Characteristics of a Good Coding Scheme**
    1. Individuality
       The code must identify each object in a set uniquely and with absolute precision. It must be used universally over the entire organization.
    2. Space
       A code number must be briefer than the description.
    3. Convenience
       It must be short, simple and consistent of digits and/or uppercase alphabets so that people can easily use them. It's better to avoid special symbols.
    4. Expandability
       As far as possible future growth in the number of objects in a set should be provided for.
    5. Suggestiveness
       The logic of the coding scheme should be readily understandable. The letter or number should be suggestive of the item characteristics.
    6. Permanence
       Changing circumstances should not invalidate the scheme or invalidation in the future should be kept to minimal.

➔ **Coding Schemes**

Following are some of the commonly used coding schemes:

1. Classification Codes
   Such codes place separate entities such as events, people or objects into distinct groups called **classes.** A code is used to distinguish one class from another. The user classifies the event into one of the several possible categories and records the code.

2. Function Codes
   These state the activities or work to be performed without spelling out all of the details in a narrative statement. Data required for input vary depending upon what function is needed.

3. Significant-Digit Subset Codes
   Here numbers are assigned in a sequence. Sometimes a prefix is added to the identification numbers to further describe the type of item. Codes can be divided into subsets or sub codes. The sub codes give the user additional information about the item.

4. Mnemonic Codes
   Such codes are suitable where the codes have to be remembered by people. E.g. DR for drills, SW for saw blades etc.
5. Hierarchical Classification

➔ **Designing Efficient Data Entry**

- The quality of data entered can be improved through attainment of 2 main data entry **objects:**
  1. Effective and efficient data capture (through a well designed form)
  2. Effective coding, and
  3. Appropriate data entry methods (using apt input devices)
- Accuracy of data entry can be enhanced through the use of input validation. Input transactions are checked to assure that they are acceptable authorized, and correct.
- Input validation includes checks for
  - Missing data,
  - Length of the data item,
  - Range and reasonableness of the data, and
  - Invalid values of data.

DATA STORAGE

- There are two approaches for storing data
  a. Conventional file approach
  b. Database approach
- Conventional File Approach: In this approach data is stored in individual files. i.e. one file for each application. Conventional files include master files, table files, transaction files, work files and report files. They can have sequential organization, random or direct organization, indexed organization or indexed-sequential organization. However when the data is to be used by multiple applications this method is inadequate.
- Database Approach: Here data is stored in a database which can be shared among users / applications as need arise.
- A separate database management staff overseas the design and development of the database.

- The systems analyst is responsible for identifying and satisfying user requirements by drawing on the data stored in the database, and developing independent master and transaction files.

DESIGN OF DATA COMMUNICATIONS

- Most information systems in practice involve the transmission of data between different locations.
- The systems analyst is responsible for :
    a. Selecting the right communication equipment,
    b. Taking the steps needed to design the application ,
    c. Specifying the method for linking the application to the communication network, and
    d. Selecting the most useful cost effective communication services.

➔ **Requirements for Data Communication System**

The system analyst must select the following components:

1. Communication channels: decisions regarding channel selection, transmission rate etc.
2. Communication control devices: decisions regarding selection of devices such as modems and network architecture to be utilized.

SYSTEM MANUAL

- The basic output of the system design is a description of the task to be performed complete with layouts and flowcharts. This is called job specifications manual / system manual. It contains:
    1. General description of the existing system
    2. Flow of the system
    3. Outputs of the existing system
    4. General descriptions of the new system
    5. Flow of the new system
    6. Output layouts
    7. Output distribution
    8. Input layouts
    9. Input responsibility
    10. Macro logic – the overall logic of the internal flows
    11. Files to be maintained
    12. List of programs

13. Timing estimates
14. Controls
15. Audit trail – it indicates the methods with which errors and defalcations will be prevented or eliminated.
16. Glossary of terms used.

REPORTING TO MANAGEMENT

After the system design is finished, the development team reports the results of these activities to the management. It should include:

1. Description of the apps and users source that lead to the system.
2. A summary of the results of the requirement analysis.
3. Design recommendation
4. Any changes in the cost and benefits of the new system
5. A plan for the remaining system development activities.

**

CHAPTER 9

SYSTEM'S ACQUISITION SOFTWARE DEVELOPMENT AND TESTING

SYSTEM'S ACQUISITION AND SOFTWARE DEVELOPMENT

ACQUIRING SYSTEMS COMPONENTS FRM VENDORS

- At the end of the design phase the organization has a reasonably good idea of the types of hardware, software and services it needs for the system being developed.
- The computer resources that can best meet the specifications established during the design phase are selected after the management has given the consent to go ahead with the project.
- The system development team often prepares a list of specific needs.
- Management also decides whether the hardware is to be purchased or leased from third party.

➔ **Procuring Computer Hardware**

- The user depends upon the buyer for support services, system design education etc. and expansion of computer installation for almost an indefinite period.
- The following points may be considered while selecting a computer system / vendor :
    1) The latest possible technology should be acquired as it facilitates future expansion.
    2) The speeds and capabilities of input/output and storage peripherals
    3) The software supplied by the manufacturer. The superiority of the software bundled along with the hardware has a huge impact in acquisition decision.
    4) Model selected should be one within a commercial series based on a long range plan for expansion.
    5) Selection of a configuration and a plan for its gradual expansion.

SOFTWARE ACQUISITION: MAKE OR BUY

- Once output and input designs are finalized, the nature of the application software requirements must be assessed by the system analyst.
- System development team decide:
    1. The type of application software products are needed,
    2. The degree of processing that the system needs to handle,
    3. The nature of systems software and computer hardware that will be most suitable for generating the desired outputs, and
    4. The functions and capabilities that the application software must possess.

- The system developers must determine whether the application software should be created in house or acquired.
- **Advantages of Application Packages**
  1. Rapid implementation
  2. Low risk – the organization knows what it's going to get for the price it has paid.
  3. Quality – developers are generally specialist in their product's niche area.
  4. Cost – cost of application software is generally lower
- **Disadvantages of Application Packages**
  1. Difficult to install
  2. Problem of undetected bugs in software
  3. Inadequate testing
     + The solution to avoid these problems is to deal with those vendors who are known to be reputable and who provide after sales support.
- **Sources of Packaged Software**
  1. Computer manufacturers
  2. Large and small software houses
  3. Computer retail sources
  4. User groups or association of users of a particular system.
- **Ways to evaluate software packages**
  1. Current users of a software
  2. Software benchmark test – it involves using the organization's transactions to assess the processing speed, user friendliness and the special features of the program .

STEPS INVOLVED IN SELECTION OF A COMPUTER SYSTEM

1. Preparation of design specifications – these mandatory specifications will constitute an overriding criterion of selection.
2. Preparation and distribution of RFP (Request for Proposal) to selected vendors
3. Analysis of proposals and elimination of inferior proposals
4. Presentation of proposals by vendors
5. Conduct further analysis
6. Accumulation of information from present users of the system
7. Conduct equipment benchmark tests
8. Selection of the equipment

VALIDATION OF VENDOR'S PROPOSALS

- Evaluation and ranking of the proposals submitted by the vendors is quite difficult, time consuming and expensive.
- **Factors to be considered towards evaluation**
    1. The performance capability of each proposed system in relation to its costs
        - The vendor system should be capable of processing the organization's data within the time frames desired management.
        - One way to test the operating efficiency of a particular system is to use a benchmark test for *Accuracy, Consistency and Efficiency*.
    2. The costs and benefits of each proposed system
        - A cost benefit analysis is conducted to ensure that cost of implementing the system is not greater than the anticipated benefits thereof.
    3. The maintainability of each proposed system
        - Maintainability refers to the ease with which a proposed system can be modified.
    4. The compatibility of each proposed system with existing system
        - Compatibility refers to the ability to implement and interface the new system with existing computer resources and software.
    5. Vendor support
        - Vendor support includes things like:
            - Training classes to familiarize employees
            - Help in implementing and testing the system
            - Assistance in maintaining the new system
            - Backup system
- **Methods of validating the proposal**
    - Vendors who fail to meet mandatory requirements will be screened out without further consideration
    - The desirable characteristics are more difficult to evaluate as vendors may
        a. Ignore them or
        b. Offer several alternatives
    - In order to evaluate the vendors' proposals, the criteria are listed in descending order of importance.
    - Following **methods** are used to validate the various proposals:
        1. Checklists
            - It's the most simple and subjective method of evaluation
            - The various criteria are put in a check list in the form of suitable questions against which the responses of various vendors are entered.
        2. Point-scoring Analysis

- The evaluation committee first assigns potential points to each of the evaluation criteria based on relative importance.
- After developing these selection criteria the evaluation committee proceeds to rate each vendor or package awarding points as it deems fit.
- The highest point total determined the winner.
- The evaluation committee must consider such issues as the company's data processing needs, it's in house computer skills, vendor reputations etc

3. Public Evaluation reports
   - Several consultancy agencies compare and contrast the hardware and software performance for various manufacturers and publish their reports in this regard.
   - This method is particularly useful where the buying staff has inadequate knowledge of computer facts.

- **Benchmarking problem for vendor's proposals**
  - Benchmarking problems for vendor's proposals are sample programs that represent at least a part of the buyer's primary computer work load
  - They include software considerations and can be current application programs or new programs that have been designed to represent planned processing needs.
  - Benchmarking problems are oriented towards testing whether a computer offered by the vendor meets the requirements of the job on hand of the buyer. Thus benchmarking problems can be applied only if job mix has been clearly specified.
  - If the job is truly represented by the selected benchmarking problems then this approach can provide a realistic and tangible basis for comparing all vendors' proposals.
  - ***Disadvantages***
    a. It takes considerable time and effort to select representative problems
    b. It requires the existence of operational hardware, software and services of systems.

- **Test problems**
  - Test problems disregard the actual job mix and are devised to test the true capabilities of the hardware, software or system.
  - If stakes are not high the organization may rely on benchmark tests performed by independent companies using general types of transactions.

SOFTWARE DEVELOPMENT

- In house software development is a painstaking process. The development of application software has to undergo a life cycle similar to one used to develop the entire system.
- **Stages in software development**

1. ***Program analysis***
   - The programmer ascertains for a particular application
     - The output required
     - The inputs available, and
     - And the processing
   - Then the programmer determines whether the proposed application can be or should be programmed at all.
2. ***Program design***
   - The programmer develops the general organization of the program as it relates to the main functions to be performed using input /output / file layouts and flowcharts.
3. ***Program coding***
   - The logic of the program outlined in flowcharts is converted into program statements or instructions.
   - Different programmers may write a program using different sets of instructions but each giving the same results.
   - The programmers broadly pursue three **objectives:**
     1. Simplicity
     2. Efficient utilization of storage, and
     3. Least processing time.
4. ***Debug the program***
   - Debugging refers to correcting programming language syntax and diagnostic errors so that the program 'compiles cleanly'.
   - ***Syntax:*** Syntax means vocabulary, punctuation and grammatical rules available in the language manuals that the programmer has to follow.
   - ***Clean Compile:*** It means that the program can be successfully converted from the source code written by the programmer into machine language instructions.
   - Steps in debugging
     1. Inputting the source program to the compiler,
     2. Letting the compiler find errors in the program,
     3. Correcting the erroneous code, and
     4. Resubmitting the program to compiler.
   - Structured walkthroughs

- It's a mental execution of the program by the programming team after examining the source text.
- A list of errors is made as each logical path is followed.
- ***Advantages***
  - Most errors are caught before any testing.
  - The team members who review the text become familiar with parts of the system.

- Testing the program
  - The programmer should plan the testing to be performed including testing all possible exceptions
  - The plan should require the execution of all standard processing logic
  - A log of test results and all conditions successful tested should be kept for future reference.
  - 'Interactive testing' allows the programmer to monitor each step required to process a program input.
- Review of the source code for adherence to standards
  - It's necessary to review each program to ensure that standards are being met.
  - Review should happen at ***two*** stages:
    - Before a 'clean compile'
    - During program testing phase

5. ***Program documentation***
   - It refers to writing of narrative procedures and instructions for users of the software.
   - User documentation should be reviewed for:
     - Parity i.e. software and system behave as the documentation indicates
     - Understandability.
6. ***Program maintenance***
   - This involves modification of various programs according to the dynamic requirements of business data processing applications.

PROGRAM DESIGN TOOLS

1. **Program Flow Chart**
   - It's the most common tool used for reviewing the design works of the system development project.
   - These flow charts depict the logical steps through which a computer program must proceed when solving a problem.
   - They often do ***not*** provide a broad view of how the program is organized.

- These are particularly useful for abstract like problems.

2. **Pseudo Code**
   - Pseudo code represents program logic in English-like statements instead of graphical symbols and flow lines as in flow charts.
   - It presents program code more closely and is more understandable than flow charts. Hence these are preferred by programmers. These are useful for designing transaction processing and information retrieval programs.
3. **Structure Chart**
   - The structure char organizes each of the programming tasks into well defined modules. The higher modules represent control portions of the program. The lower level modules do the actual task of the program.
   - They show how all the logical functions of the program fit together as a whole.
   - These charts do ***not*** give any detail of the actual program logic and the order in which various tasks are executed.
4. **4GL Tools**
   - These tools ensure that the work done with them is consistent with the other work performed by the system team.
   - The automation of manual task and internal consistency checks are two reasons due to which productivity gains result from using 4GL tools.
5. **Object Oriented Programming and Design Tools**
   - These tools provide a means of enhancing programmer productivity and of reducing the application backlogs.
   - Object oriented software design results in a model that describes object, classes and their relationships to one another.

SYSTEM TESTING

- Testing must be conducted prior to installation of an information system.
- It ***involves:***
  1. Preparation of realistic test data
  2. Processing the test data using the new equipment
  3. Thorough checking of the results
  4. Reviewing the results with future users, operators and support personnel.
- One of the most ***effective ways*** to conduct system level testing is to perform ***parallel operations*** with the existing system. Parallel operations consist of feeding both systems the same input data and comparing the data files and output results.
- One procedure to check new interactive system is to have several remote input terminals connected on line which are operated by supervisory personnel backed up by other personnel operating the old system. The outputs are checked for compatibility.

CHAPTER 10

SYSTEMS IMPLEMENTATION AND MAINTENANCE

SYSTEM IMPLEMENTATION

- System implementation is the process of ensuring that the information system is operational and then allowing users to take over its operation for use and evaluation.
- It includes all those activities that take place to convert from the old system to the new.
- Proper implementation is necessary to provide a reliable system to meet organizational requirements.
- **Aspects of Implementation**

  There are four aspects of implementation:
  1. Equipment installation
  2. Training personnel
  3. Conversion procedures, and
  4. Post implementation evaluation

1. Equipment installation

- The hardware required to support the new system is selected and ordered in time to allow for installation and testing of equipment during the implementation stage.
- **Activities involved**

  1) Site Preparation

  > An appropriate location must be found to provide an operating environment for the equipment that will meet the vendor's temperature, humidity and dust control specifications.

  > Proper procedures for acquisition and planning space lay out should be laid down in the system implementation phase.

  > *For a Micro Computer:* If the system to be installed is a micro computer little layout and site preparation work is necessary. Electric lines should be checked for safety.

  > *For a Mini Computer / Mainframe:* The Project manager should prepare rough layout, make cost estimates and get budget approved from the management.

  > *Factors to be considered For Space Planning:*

  a. Space occupied by the equipments
  b. Space occupied by people, and

c. Movement of equipment and people

> The clearance norms and requirements as specified by the vendor should be strictly adhered to.

2) Equipment Installation

> The equipment is physically installed by the manufacturer.

3) Equipment Check Out

> After installation of the equipment, the same is turned on and various 'diagnostic' and 'extensive' tests are performed to ensure that it is in proper working condition.

2. Training personnel

- Training personnel is of utmost importance because the success or failure of a system can depend on the way it is operated and used.
- A new system often involves new hardware and software and the users may not be familiar with these new technologies.
- Training is imparted through:
    a. Classes or
    b. Hands on learning
- **Training System Operators**

> System operators are responsible for keeping the equipment running as well as for providing the necessary support services.

> Their training must ensure that / include

i. They are able to handle all possible operations, both routine and extra ordinary.
ii. Fundamentals as how to turn on / off the system, how to use it and what constitute normal operation and use.
iii. Details of common malfunctions that may occur, how to recognize and correct them.
iv. A trouble shooting list that identifies possible problems and remedies as well as contact details of individuals to be contacted in the event any unexpected problem.
v. Familiarization with run procedures.

- **User Training**

> User training usually involves / includes:

i. Fundamentals as how to operate the equipment.
ii. Troubleshooting i.e. determining whether the problem was caused by the equipment or software or by something they have done in the system.

iii. Data handling activities i.e. editing data, formulating inquiries and deleting records.
iv. Minor system maintenance activities i.e. loading paper into printers, prepare disks etc.
v. Formatting and testing disks.

3. Conversion or Changeover From Manual to Computerized System

- Conversion or changeover is the process of changing from the old system (manual) to the new system.
- It requires careful planning to establish the basic approach to be used in the actual changeover.
- **Conversion Strategies**

1. *Direct Changeover*

> Conversion takes place on a specified date. From that date onwards the old system is dropped and the new system is put into use.

> *Advantage* is that Adaptation is necessary i.e. users have no possibility of using the old system after the specific date.

> *Disadvantages*

1) Long delays if errors occur as there are no other ways to process data,
2) resistance from users and
3) No adequate way to compare performance with old system.

2. *Parallel Conversion*

> This refers to running the old system and the new system at the same time, in parallel.

> This is the most common method used especially when converting from a manual system to computerized system.

> *Advantages*

1) Possibility of checking new data against old data. This helps in troubleshooting.
2) Users are not forced to convert. Hence they feel more secured.

> *Disadvantages*

1) Increased cost for running both the systems simultaneously.
2) Doubling of work load for employees.
3) Difficulty in comparing results of new system with that of old system unless the old system is a manual one.

4) Employees may prefer old system to new one if they are given choice.

3. Gradual Conversion

> In this strategy the volume of transactions is gradually increased as the new system is phased in.

> This method attempts to combine the best features of the direct changeover and parallel conversion methods.

> *Advantages*

1) Gradual conversion allows users more time to interact with new system.
2) Bugs in the new system can be discovered.

> *Disadvantages*

1) Takes too long to get the new system in place.
2) It's inappropriate for conversion of small and uncomplicated system.

4. Modular Prototype Conversion

> This approach uses the building of modular, operational prototypes to change from old system to new in a gradual manner.

> As each module is modified and accepted it's put to use.

> *Advantages*

1) Each module is thoroughly tested before its implemented.
2) Users become familiar with each module as it becomes operational.

> *Disadvantage*

1) Many times prototypes are not feasible.
2) Individually built modules may not work as a system.

5. Distributed Conversion

> This refers to a situation in which many installations of the same system are contemplated.

> System is first implemented in one or two branches and if it becomes successful the whole network is converted to new system. E.g. banking

> *Advantage* is that the problems can be found out early.

> *Disadvantage* is that each site has its own peculiarities to work through.

- **Activities Involved in Conversion**

1. ***Procedure Conversion***
   - > Operating procedures for personnel in both functional and computer – operations areas should be clearly defined before system conversion.
   - > Written operating procedures must be supplemented by oral communication during the training sessions on the system change.
   - > Brief meetings must be held when changes are taking place in order to inform al operating employees of any change initiated.
   - > Revisions to operating procedures should be issued as quickly as possible.
   - > Once the new system is completely operational, channel of communication between system development team and supervisory personnel should be opened so that necessary changes can be initiated as conditions change.

2. ***File conversion***
   - > This phase should actually be started long before programming and testing are completed.
   - > The cost and related problems of file conversion are significant irrespective of file types.
   - > Present manual files are likely to be inaccurate and incomplete.
   - > *Compatibility issues:* If the existing system is operating on a computer but of a different configuration, the formats of the present computer files may be unacceptable (not compatible) for the new system
   - > The files may require character translation that is acceptable to the character set of the new system.
   - > Rearrangement of certain data fields for more efficient programming may be desired.
   - > *Precautions on File Conversion*
     1) File conversion programs should be thoroughly tested to ensure accuracy.
     2) Adequate controls like record count should be inserted into such programs.
     3) The original files should be kept as backup for a reasonable period.

3. System Conversion

> At this stage, daily processing is shifted from the existing information system to the new one.

> A cut-off date is established so that database and other data requirements can be updated to the cut-off point. All transactions initiated after this time are processed on the new system.

> Consideration should be given to operating the old system for some more time to permit checking and balancing the total results of both systems. Any differences should be reconciled.

> The old system can be dropped as soon as the data processing group is satisfied with the new system's performance.

4. Scheduling Personnel and Equipment

> Scheduling data processing operations of a new system for the first time is a difficult task for the system manager.

> Schedules should be set up by the system manager in conjunction with departmental managers of operational units serviced by the equipment.

> The *Master Schedule* for next month should provide sufficient computer time to handle all required processing.

> *Daily Schedules* should be prepared in accordance with the master schedule and should include time necessary for returns, program testing, special reports and other runs.

> Scheduling an interactive system is more difficult than scheduling a batch processing system.

5. Alternative Plans In Case of Equipment Failure

> Alternative processing plans must be implemented in case of equipment failure.

> Priorities must be given to critical jobs in an organization. E.g. billing.

> *Documentation*

- It's the responsibility of the computer section and should be fully covered by the organization's systems and procedures manual.
- *Contents*

a. Critical jobs

b. How to handle these jobs during down time

c. Location of compatible/backup equipment

d. Persons responsible for each area

e. Deadlines to be met during emergency

4. <u>Post implementation evaluation</u>

- The final step of the system implementation is evaluation.
- It provides the feedback necessary to assess
  a. The value of information, and
  b. The performance of personnel and technology included in the newly designed system.
- **<u>Functions of Feedback</u>**

  Providing information as to what adjustments
  a. May be necessary to the information system
  b. Should be made in approaching future information systems development projects.
- **<u>Dimensions of Evaluation</u>**
  > There are *two* basic dimensions of information system evaluation:
  1. Whether the system is operating properly, and
  2. Whether the user is satisfied with its performance.

  > ***Development Evaluation***
  - It's primarily concerned with whether the system was developed on schedule and within budget.
  - It requires schedules and budgets to be established in advance and that record of actual performance and cost be kept.

  > ***Operation Evaluation***
  - It pertains to whether the hardware, software and personnel are capable to perform their duties and whether they actually perform.

  > ***Information Evaluation***
  - Information evaluation is very difficult and it cannot be conducted in a quantitative manner.
  - Here the extent to which information provided by the system is supportive to decision making is the area of concern in evaluating the system.
  - However it's practically impossible to evaluate this aspect.
  - *<u>Nolan and Seward Method (Richard L Nolan and Henry H Seward)</u>*
    - Under this approach the information system is evaluated on the basis of user satisfaction.
    - The more frequently a decision maker's information needs are met by the system, the more satisfied he tends to be with the system.

SYSTEM MAINTENANCE

- Most information systems require at least some modification after development.
- **Need For Modification**
    1. Failure to anticipate all requirements during system design, and/or
    2. Changing organizational requirements
- System maintenance involves adding new data elements, modifying reports etc.
- **Categories Of Maintenance**
    1. Schedule Maintenance which is anticipated and planned for, and
    2. Rescue Maintenance to rectify previously undetected malfunctions.
- An information system may remain in an operational and maintenance mode for several years.

**

CHAPTER 11

DESIGN OF COMPUTERISED COMMERCIAL APPLICATIONS

COMPONENTS OF ACCOUNTING INFORMATION SYSTEM

1. **General Ledger System**
    a. General ledger
    b. Budgeting
    c. Responsibility/profitability reporting
2. **Cash receipts/disbursement system**
    a. Accounts payable & receivable
    b. payroll
3. **Production management system**
    a. Material inventory control
    b. Work in progress control
    c. Cost estimation, and
    d. Production scheduling system
4. **Marketing system**
    a. Finished goods inventory control
    b. Order processing, and
    c. Marketing analysis systems

ACCOUNTS PAYABLE

- The purpose of an accounts payable system is to pay for merchandise or services received from vendors.
- **Objectives of the system**
    1. Determining when to pay and what to pay,
    2. Providing management with a way of allocating available cash, and
    3. To allow evaluation of company vendors.
- **Disbursement Voucher**
    - Every vendor submits a different form of invoice.
    - So vital information is extracted by hand from each invoice and this information is recorded on a standardized document called a Disbursement Voucher.
    - The disbursement voucher stapled along with the invoice it represents is sent to data entry department for input of data.

PAYROLL ACCOUNTING

- Payroll is one of the oldest and most common business computer applications.
- The basic purpose of the payroll system is to produce pay slips and pay cheques for the employees every month.
- It requires collecting employee work hours through their attendance cards, converting hours to gross earnings and computing deductions and net pay.
- Other activities of payroll includes:
    a. Accumulating summary data for general ledger reports
    b. Printing quarterly and year end reporting statements
    c. Making labor distribution and job costing/performance measurements and reporting them

FINISHED GOODS INVENTORY CONTROL

- Inventory management seek to retain only enough inventory to meet the demand for stock , to never run out of stock and to allow economic lots of stock to be purchased as well as carried in inventory.
- **Objectives of the System**
    1. To provide high quality service to customers
    2. To minimize the amount of money invested in inventory and money required to cover inventory carrying cost.
    3. To provide management with information needed to help achieve the two preceding objects.

SALES ORDER PROCESSING SYSTEM

- The sales department prepares the sales bill in duplicate upon the receipt of the customer's purchase order after satisfying that the customer's account is not delinquent.
- An Online real time (OLRT) system can fully process a transaction as soon as it's entered.

MATERIAL INVENTORY CONTROL

- Materials inventory control system is the point at which materials enter the manufacturing accounting system.
- This system controls inventory and minimizes the costs of purchasing and holding inventory shortages.

WORK IN PROCESS CONTROL

- This system assigns materials, labor and overhead costs to production jobs or products.
- **Objectives of the system**
  1. To cost jobs through the manufacturing process
  2. To provide management with information to assist in controlling costs, and
  3. Measuring the performance of departments or other units within the factory.

COST ESTIMATION

- Cost estimation system provides with manufacturing cost estimates based on inquiries received from potential customers.

PRODUCTION SCHEDULING

- Production scheduling is the nerve centre of the production management system. It schedules production and monitors all physical flows.

FINANCIAL ACCOUNTING

- It's concerned with
  - the preparation of balance sheet and P&L account
  - entering all transactions and keeping track of the balances of the various account heads.

- Financial accounting is an area which is extremely amenable to computerization. All processing is well defined and numerical.

SHARE ACCOUNTING

- A share accounting system needs to maintain an updated list of shareholders.
- When a person purchases shares from a shareholder, a share transfer form along with the certificates is sent by the buyer to the company for incorporating the transfer.
- The system records a change in ownership for the shares.
- **Facilities provided by a Share accounting System**
  1. Recording share transfer
  2. Issuance of dividend warrants
  3. Bank mandate facility if warrants are to be sent to shareholder's bank
  4. Splitting of share certificates
  5. Consolidation of shares
  6. Mailing annual reports and invitations to various meetings.

**

CHAPTER 12

ENTERPRISE REOURCE PLANNING: REDESIGNING BUSINESS

ERP: THE CONCEPT

- ERP is a standard software package, which equips the enterprise with necessary capabilities to integrate and synchronize the isolated functions into streamlined business process in order to gain a competitive edge in business environment.
- ERP software package offers an integrated software solution to all functions of an organization.
- ERP solutions seek to streamline and integrate operation processes and information flows in the company to synergies the resources of an organization namely men, money and machine through information.
- It provides an integrated information storehouse where information needs to be stored only once and can be further processed and reported to anyone in the value chain.
- **Definition**
  - It's a fully integrated business management system covering functional areas of an organization. It organizes and integrates operation processes and information flows to make optimum use of resources.
  - It's a global, tightly integrated closed loop business solution package.
  - ERP promises one database, one application and one user interface for the entire enterprise.
  - A modern ERP system enhances a manufacturer's ability to accurately schedule production, fully utilize capacity, reduce inventory and meet promised shipping dates.
- **Evolution of ERP**
  - ERP has evolved from system known as MRP II (Manufacturing Requirement Planning). It's a method for planning of all the resources of the manufacturing company and involves all operational and financial planning and has simulation capabilities.
  - Its major drawback is that it cannot effectively integrate the different functional areas to share the resources effectively.
  - MRP II evolved from MRP (Material Requirement Planning) Systems
  - MRP is considered as an important planning and manufacturing control activity for materials.
- **Enabling Technologies**
  - Most of the ERP systems use three tier client server architecture.
  - To facilitate online data transfer ERP systems user such technologies like group ware, EDI, internet etc.

- **ERP characteristics**
    1. Flexibility – flexible to respond to changing needs of an enterprise.
    2. Modular & Open – ERP systems should have an open system architecture i.e. any module can be interfaced or detached whenever required without affecting other modules.
    3. Comprehensive – should be able to support variety of organizational functions
    4. Beyond the company – should support on-line connectivity with other business entities.
    5. Best Business practices – must have a collection of the best business practices.
- **Uses/benefits of ERP**
    1. Supports strategic planning, operational planning, execution activities and creation of materials and resources.
    2. Involves end to end Supply Chain management
    3. Facilitates companywide integrated information system
    4. bridges the information gap across organizations
    5. it's the solution for better project management
    6. allows automatic introduction of latest technologies
    7. Provides intelligent business tools like DSS.
    8. Reduce paper documents
    9. Improved timeliness
    10. Cost control
    11. Faster response and follow up to queries
    12. Better monitoring
    13. Provides a unified customer database
    14. Improves international operations
    15. Improved information access
    16. Greater accuracy of information.

BUSINESS PROCESS RE-ENGINEERING (BPR)

- Every company that intends to implement ERP has to re engineer its processes in one form or the other. This is known as BPR.
- **Definition by Hammer and Champhy**: BPR is the *fundamental rethinking* and *radical redesign* of the processes to achieve *dramatic improvement* in critical contemporary measures of performance such as cost, quality, service and speed.
    - *Fundamental rethinking:* involves eliminating business processes if it does not add any value to the customer.
    - *Radical redesign:* means reinventing and not enhancing or improving.
    - *Dramatic improvement:* means a reduction of 80%-90% of costs and processing time.

- Thus BPR aims at major transformation of the business processes to achieve dramatic improvement.
- The business objectives of the enterprise are achieved by transformation of the business processes which may or may not require the use of Information technology.
- **Business engineering**
  - Business engineering has come out of merging of two concepts namely Information technology and BPR.
  - It's the rethinking of business processes to improve sped, quality and output of materials and services. It's a method of development of business processes according to the changing requirements.
  - It's based on the concept of Process Oriented Business Solutions enhanced by the Client Server computing.
  - The main point in business engineering is the efficient redesigning of company's value added chains (series of connected steps running through a business which when efficiently completed add value to the enterprise and cutomers)
- **Business Management**
  - The basic objective of implementing ERP is to put in place the applications and infrastructure architecture that effectively and completely support the enterprise's business plan and business processes.
  - The first step in implementation of ERP is the development of a Business Process Model.
- **Business Modeling**
  - It involves creation of a model consisting of core business processes or activities. It is a diagrammatic representation of business as a large system with interconnection of subsystems or processes that it comprises of.
  - A reference model can be used by companies to list down their business processes and data entities and if required can be subsequently modified to suit the specific nature of requirements.
- **Business Modeling in Practice**
  - Most of the ERP packages available enable flow charting of business processes using standard flow chart symbols. E.g. SAP uses Event driven Process Chain (EPC) methodology to model business processes.
  - ERP packages also provide a standard Template for each of the processes so that actual processes can be compared and deviations analyzed.
  - Thus using a business model it's possible to check as t how well the model fits into the application so that the degree of suitability of ERP package can be assessed.

ERP IMPLEMENTATION

- ERP brings together in one platform, different business functions, personalities, procedures, ideologies and philosophies with an aim to pool knowledge base to effectively integrate and bring worthwhile and beneficial changes throughout the organization.
- ERP implementation involves considerable amount of time, efforts and valuable resources and the success is not guaranteed. Hence it's a risky affair.
- The success of the implementation mainly depends upon how closely the implementation consultants, users and vendors work together to achieve the overall objectives of the organization.
- After implementation, ERP package is expected to improve the flow of information and formalize & standardize business processes and workflow that exist in the organization.
- However it may be noted that implementation of ERP may not necessarily result in reduction of work load.
- ***Customization:*** It refers to making changes in a standard ERP package to suit specific needs of the enterprise at the time of implementation. It should be kept in mind that maximum benefit will be available only when the standard package is implemented in totality.
- The roles and responsibilities of the employees have to be clearly identified, understood and configured in the system.
- Moreover the ERP package should be expandable and adaptable to meet the dynamically changing business processes.
- A well implemented ERP package can give a 200% return where a poorly implemented system gives only 25%.
- **ERP Implementation Methodology / Steps In ERP Implementation**
    1. ***Identifying the Needs For Implementing the ERP Package***
        - This involves the reasons for implementing the ERP package and evaluating the profitability of installing an ERP system.
    2. ***Evaluating the 'As Is' Situation of the Business***
        - Understanding the present situation of the business, the various functions and business processes used to achieve business transactions.
    3. ***Deciding the Desired 'Would Be' Situation***
        - This involves optimizing processes using tools like *benchmarking* to ensure that processes achieved are the best in industry.
    4. ***Reengineering the Business Process***
        - BPR is done to
            - Reduce the business process cycle time
            - Reduce the number of decision points to minimum, and
            - Streamline the flow of information and eliminating unwanted flows.

5. ***Evaluation of Various ERP Packages***
    - Criteria for evaluation of ERP packages are:
        - Flexibility
        - Openness
        - Integration
        - Beyond the company
        - Best business practices
        - Global and local presence of the package
        - Price
        - Ease of implementation
        - Post implementation support etc
6. ***Finalization of ERP Package***
    - ERP package finalization is done after comparing critical features of each package.
7. ***Installation of Hardware and Networks***
8. ***Finalizing the Implementation Consultants***
    - Criteria for selection of consultants are:
        - Skill set
        - Industry specific experience
        - Cost of hiring
9. ***Implementation of ERP Package***

- **Implementation Guidelines**
    1. Adopt an implementation strategy to match corporate needs and culture
    2. Undertake a business process redesign exercise prior to implementation
    3. Establish a good communication network
    4. Provide strong and effective leadership
    5. Appoint a capable project manager
    6. Form a balanced team of implementation consultants
    7. Select good implementation methodology
    8. Train end users
    9. Adapting to the new system.

POST IMPLEMENTATION: EXPECTATIONS, FEARS AND REALITIES

- Many post implementation problems can be traced to wrong expectations and fears that the corporate management has from an ERP.
- During implementation phase the expectations, fears and reality are balanced.
  - **Expectations**
    - Improvement in processes
    - Total automation
    - Increased productivity
    - Elimination of manual reports
    - Availability of real time information system
  - **Fears**
    - Job redundancy
    - Change in job profile
    - Fear of loss of authority
    - Increased stress
  - **Realties**
    - Changing the organization requires a mindset change
    - Measurement of key performance indicators
    - Processes peculiar to some sectors and organization should be kept out of the ERP package
    - Some processes are better done manually
    - Changing the organization involves 3 levers: strategic, business process and consequential organizational change.
    - ERP implementation is not the end of the road as far as change is concerned.
- **Life after Implementation**
  - Change integration has to be embedded in the task list for any ERP implementation.
  - This can be achieved through the process of communication i.e. educating all layers of management on the particular ERP product, it's relevant functionlaity, limitations and benefits.
  - Critical Success Factors (CSFs) for the company as a whole as well as for respective functionalities or departments should be listed out.
  - Key Performance Indicators (KPIs) required to address these CSFs should also be established.
  - The processes to be configured on an ERP should also be decided at the start of project.

- **Resolving Post-Implementation Blues**
  - The major task after implementation is to monitor KPIs and take correct business decisions to improve them.
  - There should be strong management resolve to implement the system.
  - There will be need for course correction many times during post implementation.
  - ***Reasons For Course Correction***
    - Change in business environment.
    - A review indicates a need for change in some processes
    - Vision changes
    - Additions to business which require extra functionality
  - The international trend is to outsource the activity of maintenance and up gradation to enable the company to concentrate on its business activity.
  - The management should ensure proper usage of the system by integrating the business objectives with the ERP functionality during implementation.
  - Periodic ERP Audits by independent agencies will help the management to evaluate security, authorization controls and other key areas of the system and to improve the existing setup.

SOME ERP VENDORS

- The Baan Company (Baan)
- Business Planning and Control Systems
- Marcam Corporation(Mapics XA, Prism)
- QAD (MFG/Pro)
- Oracle (Oracle Applications)
- SAP (R/3)
- JBA (System 21)

SAP ERP PACKAGE

- SAP AG has developed an ERP package called SAP.
- SAP has a number of application modules which in turn has several components. Modules are discussed below.

1.Financials

- Financial Accounting
  - General Ledger
  - Account Receivable & Payable
  - FA Accounting

2. Controlling Cost

- Overhead Cost Control
- Cost Centre Accounting
- Overhead Orders
- Activity based Costing
- Product Cost Control
- Cost Object Controlling
- Profitability Analysis : examining sources of returns

3. Investment Management

- Corporate wide Budgeting
- Appropriation requests
- Investment Measures
- Automatic Settlement to FA (Capitalization of WIP)
- Depreciation Forecast

4. Treasury

- Cash Management
- Treasury Management
- Market Risk Management: it's a process which involves a complex feedback loop encompassing data collection, risk measurement, analysis and simulation as well as active planning of financial instruments. This component provides various measurements for analyzing and assessing interest rates and currency risks, market to market.
- Funds Management

5. Integrated Enterprise Management (Enterprise Controlling)

- EC – CS
- EC – PCA
- EC – EIS

6. Product Data Management (PDM)

PDM Supports in creating and managing product data throughout product life cycle.

7. Sales & Distribution

This module supports access to real time, on line information from sales support to the billing process.

- Shipping Management System

- Transport Module
- Foreign Trade Processing
- Billing
- Sales Information System

8.Production Planning & Control

- Sales and Operation Planning (SOP)
- Production Control Modules
- Quality Management
- Project System
- Project Information System

9.Materials Management

- Purchasing
- Inventory Management
- Warehouse Management
- Invoice Verification
- Inventory Control using Purchase Information System
- Quality Management
- Plant Maintenance
- Service Management

10. Human Resource Management

- Personnel Administration
- Employee Master Data
- Recruitment Management
- Open Positions
- Selection And Hiring
- Travel Management
- Benefits Administration
- Personnel Cost Planning

11. Payroll Accounting

- Payroll Processing
- Integration
- Global Solution
- Time Management

- Time Data
- Time Evaluation
- Time Management Review
- Integration And Interfaces
- Shift Planning

12. Internet & Intranet

- SAP Business Workflow
- Employee Self Service

**

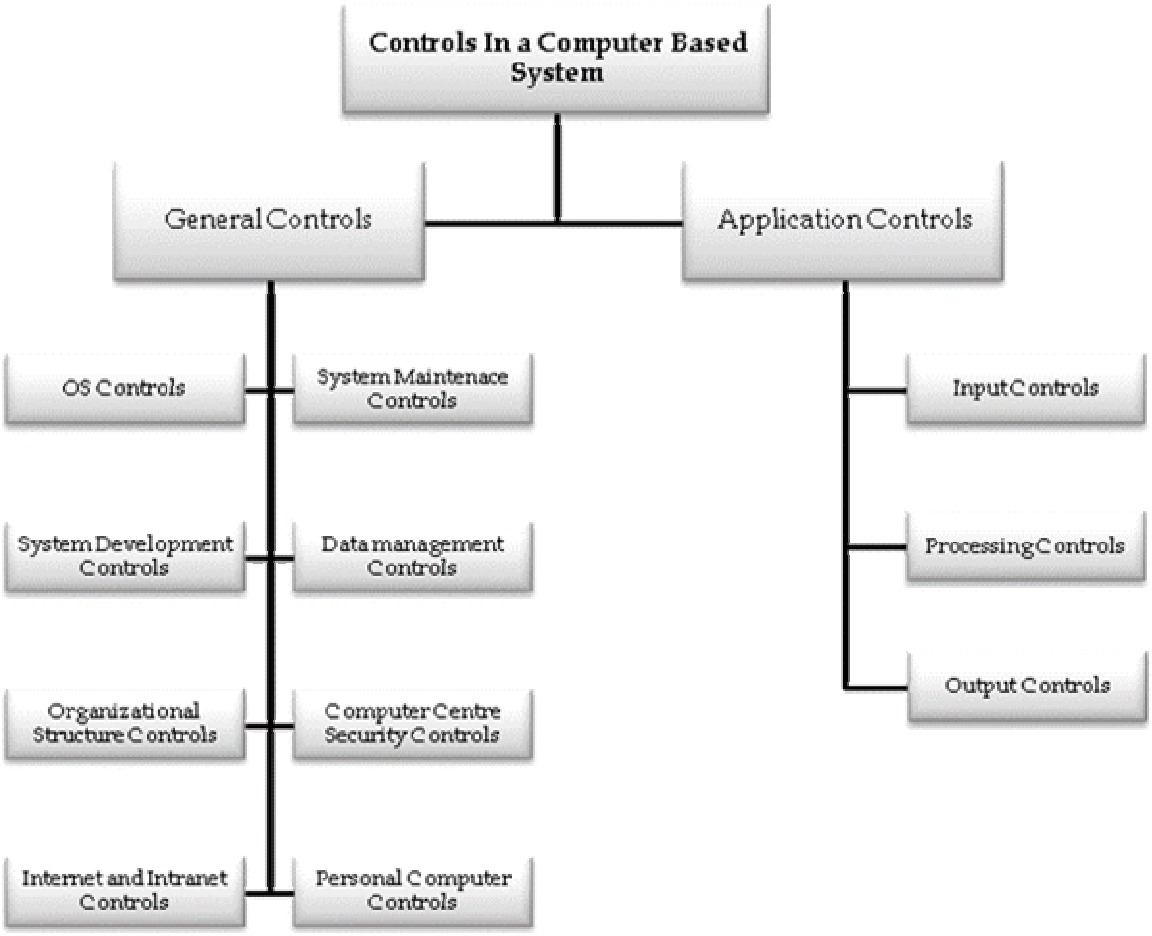
CHAPTER 13

CONTROLS IN EDP SET-UP: GENERAL CONTROLS

INTRODUCTION

- Controls for the electronic data processing system are even more important than they are for a manual one.
- **Importance of Control: Reasons**
    1. An EDP system is likely to process more information than a manual system. Hence the potential for errors is also very high.
    2. EDP systems gather, process and store activity data in forms which are not human readable, and
    3. EDP systems have blurred audit trail.

TYPES OF CONTROLS IN A COMPUTER BASED SYSTEM



1. **General Controls**
   These controls apply to a wide range of expressions that systematically threaten the integrity of all applications processed within the Computer Based Information System (CBIS). Following are the sub divisions of general controls:
2. **Application Controls**
   These are focused on exposures associated with specific systems such as payroll, Accounts receivables etc.

GENERAL CONTROLS

OPERATING SYSTEM CONTROLS

- Operating System allows users to share and access common computer resources. It's the computer's control program.
- If OS's integrity is compromised, controls within individual accounting applications may be neutralized.
- Since the OS is common to all users, the larger the computer facility, the greater the scale of potential damage.
- **Tasks performed by Oss**
  - Translating high level languages into machine level languages
  - Allocating computer resources to users
  - Job Scheduling and multiprogramming
- **Control Objectives**
  To perform the above mentioned tasks reliably and consistently, the OS should achieve following control objectives.
  1. The OS should protect itself from users and user applications.
  2. The OS must protect users from each other (hacking).
  3. The OS must protect users from themselves (one module of an application may destroy another module of the same program).
  4. The OS should be protected from itself.
  5. The OS should be protected from its environment (shutting down the system in the event of power failure or other mishaps so that it can recover later)
- **Operating System Security (Security Components in OS)**
  - ***Log on Procedure***
    > Log on procedures is used to restrict access to the system. It's the first line of defense against unauthorized access.

> When a user initiates a process, he or she is presented with a dialogue box requesting user ID and password. Access is granted only if a matching User ID and password is submitted.

- ***Access Tokens***
  > If the log on attempt is successful, the OS creates an access token that contains key information about the user like user ID, password, user privileges etc.
  > The information in the access token is used to approve all actions attempted by the user during the session.
- ***Access Control Lists***
  > It contains information that defines the access privileges for all valid users of the resource
- ***Discretionary Access Control***
  > The system administrator determines who is granted access to specific resources and maintains the access control list.
  > In distributed system resources may be controlled by end users and in this case they may be granted discretionary access control which allows them to grant access privileges to other users.

➢ **Threats to OS Integrity**

- OS control objectives are sometimes not achieved due to lows in the OS that are exploited accidently or intentionally.
- ***Accidental Threats***
  > These include hardware failures that cause the OS to crash, errors in user application.
  > Such failures may cause memory to be 'dumped' to disks which may result in unintentional disclosure of sensitive information.
- ***Intentional Threats***
  > Such threats include attempts to illegally access data or violate user privacy for financial gain.
  > Sources of such threats are:
    1. Privileged personnel who abuse his authority.
    2. Individuals who browse the OS to identify and exploit security flaws.
    3. Users who insert computer Viruses or other Malware applications.

➢ **Controlling Access Privileges**

- Privileges determine which directories, files, applications and other resources an individual or group may access.
- Privileges should be carefully administered and closely monitored for compliance with organizational policy and principles of internal control.

- **Various Methods**
  - > ***Password Control:*** A password is a secret code entered by the user to gain access to system, application etc.
  - > ***Reusable Passwords:*** The user defines a password to the system once and then uses it to gain future access. The quality of the security provided by a reusable password depends on the quality of the password.
  - > ***One-time Passwords:*** Here the user's password changes continuously. To gain access the user must provide both a secret reusable PIN and the current one time only password for that point in time.

➢ **Controlling Against Viruses and Other Destructive Programs (Malware)**

- **Virus**
  - > A virus is a destructive program that attaches itself to a legitimate program to penetrate the OS.
  - > It destroys application programs, data files and the OS.
  - > A virus may attack in a variety of ways:
    1. Replicating itself over and over within the main memory thus destroying whatever data / programs resident are in memory.
    2. Spreading through the network to other systems.
  - > A virus commonly attach itself to following types of files:
    1. .exe /.com / .ovl program files
    2. Boot sector of a disk
    3. A device driver program
- **Worm**
  - > A 'Worm' is a program that 'burrows' into the computer's memory and replicates itself into areas of idle memory.
  - > The main difference between a virus and a worm is that the replicated worm modules remain in contact with the original worm that controls their growth. The replicated virus modules grow independently of the initial virus.
- **Logic Bomb**
  - > It's a virus / worm that is triggered by some predetermined event like a particular date. E.g. Michelangelo Virus.
- **Back Door (Trap Door)**
  - > It's a software program that allows unauthorized access to a system without going through the normal (front door) log on procedure. Such back doors are usually created by the programmers.
- **Trojan Horse**
  - > Trojan horse is a program that captures the user IDs and passwords from unsuspecting users by mimicking normal log on procedures of the OS.

> When the user enters his ID and password the Trojan horse stores a copy of the same in a secret file.

- **Ways to Control Threats From Malware**
  1. Purchase software only from reputed vendors
  2. Examine all software updates for viruses before installing
  3. Conduct educational programs to raise user awareness
  4. Test all new application software with anti-virus software.
  5. Routinely make backup copies of key files
  6. Use anti-virus software which scans the system for possible virus infections.

➢ **Controlling Audit Trails**

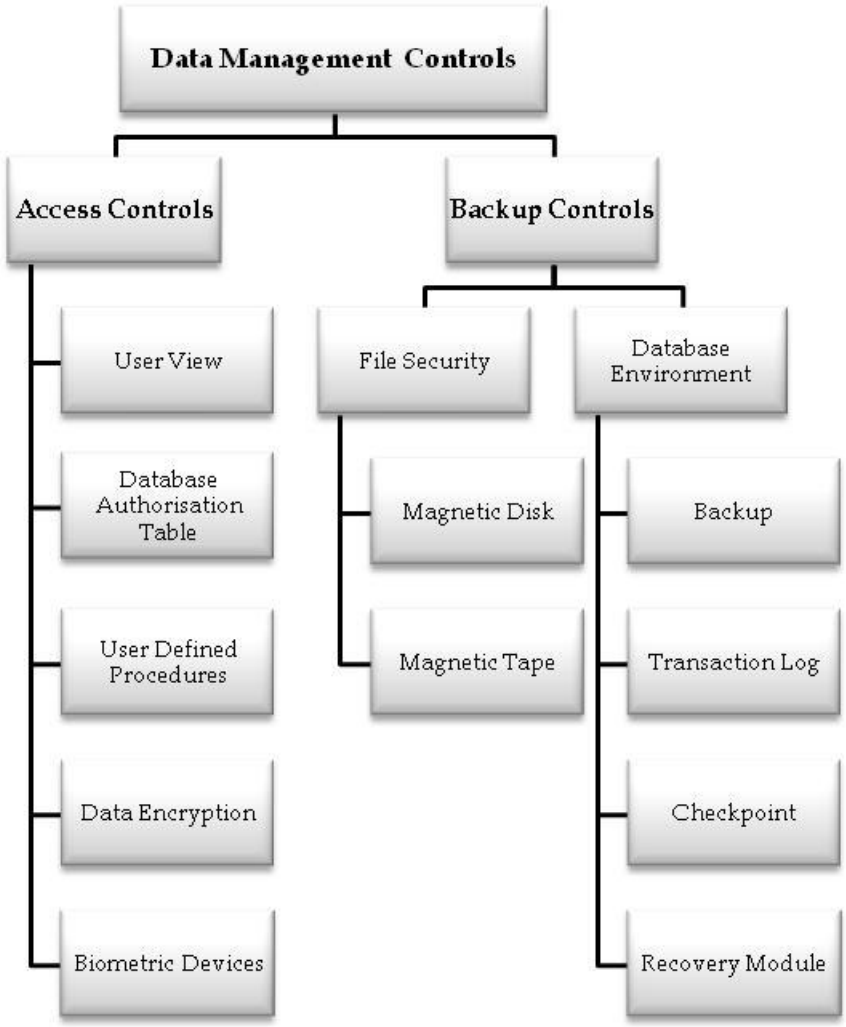
- Audit trails are logs that can be designed to record activity at the system, application and user level. They provide an important detective control to help accomplish security policy objectives.
- An effective audit policy will capture al significant events without cluttering the log with trivial activity.
- **Audit Trail Objectives / Uses**
  > ***Detecting Unauthorized Access***
    - Real-time detection
      a. To protect the system from outsiders who are attempting to breach system controls, and
      b. To report changes in system performance that may indicate infestation by a virus or worm
    - After-the Fact detection: such trails are used to determine if unauthorized access was accomplished or attempted and failed.

  > ***Facilitating Reconstruction of Events***
    - Audit trails can be used to reconstruct the steps that led to events such as system failures, security violations or application processing errors.

  > ***Promoting Personal Accountability***
    - Audit trails can be used to monitor activity at the lowest level of detail. This is a preventive control that can be used to influence behavior.
- **Implementing an Audit Trail**
  > Audit trails can be used to measure the potential damage and financial loss caused by security violations.

  > It also provides valuable evidence for assessing the adequacies of controls in place.

DATA MANAGEMENT CONTROLS



1. Access Controls

- Access controls are designed to prevent unauthorized individuals from viewing, retrieving, corrupting or destroying data.
- Access controls can be effectively implemented in a Flat File System Environment where users maintain exclusive ownership of their data. When a file is not in use it's closed and taken off line and physically secured in Data Library.
- However in a Shared Database environment access control risks are much greater as files are always kept on-line. Following are some database control features:

1. User View (Sub Schema)

- It's a subset of the total database that defines the user's data domain and provides access to the database.
- The DBA is responsible for user view design.

- Access privileges to data, as defined in their views, should be adequate with users' legitimate needs.
- User views thus can restrict user access to a limited set of data. However, they do not define task privileges such as read, write or delete.

2. Database Authorization Table

- Database authorization table contains rules that limit the actions a user can take (similar to access control list).
- Each user is granted certain privileges that are coded in the authorization table which is user to verify the user's action requests.
- Each row in the table indicates the level of action i.e. read, write, delete or edit.

3. User defined procedures

- It allows the user to create a personal security program or routine to provide more positive user identification than a single password can. E.g. series of personal questions.

4. Data Encryption

- Data encryption uses an algorithm to scramble selected data thus making it unreadable to an intruder 'browsing' the database.
- Databases use encryption procedures to protect:
  - Highly sensitive data in the database, and
  - Data transmitted across network.

5. Biometric Devices

- Here biometric devices are used to measure various personal characteristics (like fingerprint) to validate authorization.
- The user characteristics are digitized and stored in a database security file or on ID card that the user carries.
- When an individual attempts to access the database, a special scanning device captures his biometric characteristics and compares to profile data. Access is granted if both match.

2. Backup Controls

- Data can be corrupted and destroyed by malicious acts or natural calamities.
- To recover from such disasters, organizations implement policies, procedures and techniques that systematically and routinely provide backup copies of critical files.

1. The File Security

The techniques employed for reconstruction of master files on magnetic disks and tapes in the event of data loss.

1. *Magnetic Disk*
   - Contents of master file in magnetic disk are periodically copied on magnetic tape backup file and stored at another location.
   - A separate record of transactions is maintained for :
     a. Providing a link from one backup file to another, and
     b. Providing particulars of all records that caused a change to the magnetic disk file.
   - In the event of data loss data from magnetic tape and transaction record file are used to reinstate the master file.
2. *Magnetic Tapes*
   - The procedure followed in reconstruction of files in case of magnetic tapes is referred to as ***Generation Technique*** as files relating to two previous records are retained to the current updated master file and the current transaction file.
   - Procedure:
     a. The master file produced is called the *son* tape.
     b. The son tape produced during the updating run replaces the first *son* tape which becomes the *father* tape.

     This procedure is repeated again.

2. *Database Environment*

Most DBMSs have a backup and recovery system. Such systems provides for following recovery features:

1. *Backup*
   - It makes periodic backup of the entire database (Automatic procedure).
2. *Transaction Log*
   - It provides an audit trail of all processed transactions. It records all resulting changes to the database in a separate database change log.
3. *Checkpoint*
   - Checkpoint suspends all data processing while the system reconciles the transactions log and database change log against the database.
   - Checkpoints occur automatically several times in an hour.
4. *Recovery Module*
   - It uses the logs and backup files to restart the system after a filure.

ORGANIZATION STRUCTURE CONTROLS

- **Manual System**

  In a manual environment operational tasks must be separated to:

  1. Separate the task of transaction authorization from transaction processing
  2. Separate record keeping from asset custody
  3. Divide transaction-processing tasks among individuals.

- **CBIS System**
  - In a CBIS system all the transactions are performed by computer programs and hence the focus of segregation control shifts from operational level to higher level organizational relationships within the computer services function.

- **Segregation of Duties within a Centralized Organization**

  1. ***Separating Systems Development from Computer Operations***
     - The relationship between system development and operations groups should be extremely formal and their responsibilities should not be combined.
     - Consolidating these functions invite fraud.
     - With detailed knowledge of the application logic and control parameters an individual can make unauthorized changes to the application.
  2. ***Separating the Database Administrator from Other Functions***
     - The DBA is responsible for a number of critical tasks relating to database security.
     - Hence the DBA functions should be organizationally independent.
     - There should be separation of the DBA function from system development also.
  3. ***Separating New System Development from Maintenance***
     - System development function can be divided into 2 groups: System analysis and Programming.
     - In System analysis phase, analysts works with users to produce a detailed design of the system and programming group code the program according to these specifications.
     - The programmer who codes the system is usually responsible for maintaining it. This approach promotes two types of control problems: inadequate documentation and fraud.
       - ***i.*** *Inadequate documentation: Reasons for Inadequate documentation*
         1. Documenting a system is not as interesting as designing, testing and implementing, and

2. Job security of the programmer as he becomes indispensible

ii. *Program Fraud*

When the original programmer of a system also has maintenance responsibility, the potential is increased.

- ***Counter Measure***

  Creation of a system maintenance group to carry on system maintenance activities after the system is implemented. I.e. system maintenance task is segregated from system development task.

4. Separating the Data Library from Operations

- The data library is usually a room adjacent to the computer center that provides safe storage for the off-line data files like removable disks.
- Data librarian must keep a detailed log of each file including file name, serial number, contents and creation & retention date.
- Access to library should be controlled by data librarian.
- The separation of the librarian from operations is important for the physical security of off-line data files.

SYSTEM DEVELOPMENT CONTROLS (Controlling New System Development Activities)

1. **System Authorization Activities**
   - All systems must be properly authorized to ensure their economic justification and feasibility. System authorization should be formal.
2. **User Specification Activities**
   - Users must be actively involved in the system development process.
   - Users can create detailed written descriptions of the logical needs that must be satisfied by the system.
3. **Technical Design Activities**
   - The technical design activities in the SDLC translate the user specifications into a set of detailed technical specifications of a system that meets users' needs.
   - It includes system analysis, general systems design, feasibility analysis and detailed system design.
4. **Internal Audit Participation**
   - Internal auditor should be involved from the inception of the SDLC process to make conceptual suggestions regarding system requirements and controls.
   - Auditor's involvement should continue throughout all phases of the development process and into maintenance phase.

5. **Program Testing**
    - Though it's time consuming, all program modules should be thoroughly tested using carefully selected test data, before implementing the same.
    - Test data should and the results should be preserved for future use to facilitate efficient implementation of audit objectives.
6. **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 users, system professionals and internal audit personnel should subject the system to rigorous testing.

SYSTEMS MAINTENACE CONTROLS

- On implementation, the system enters the maintenance phase of the SDLC.
- System don't remain static during this period, they undergo substantive changes.

1. **Maintenance Authorization, Testing and Documentation**
    - Post implementation access to system via maintenance activities increases the possibility of system corruption.
    - Logic may be corrupted either by the accidental introduction of errors or intentional acts to defraud.
    - To minimize such exposures, all maintenance activities should require minimum four controls:
        a. Formal authorizations,
        b. Technical specifications,
        c. Testing, and
        d. Documentation updates.
    - When maintenance causes extensive changes to program logic, additional controls should be invoked.
2. **Source Program Library controls**
    - ***Source Program Libraries*** are used to store (In larger computer systems) application program modules in source code form on magnetic disks.
    - *Worst Case Situation (No Controls)*
        a. Access to program is completely unrestricted and there is no provision for detecting an unauthorized intrusion.
        b. With no provision for detecting unauthorized access to SPL, the program's integrity cannot be verified.

- *Controlled Environment*
  - A SPL management program is used to protect the SPL.
  - The software is used to control four routine but critical functions:
    1. Storing programs on the SPL
    2. Retrieving programs for maintenance purposes
    3. Deleting obsolete programs from the library, and
    4. Documenting program changes to provide an audit trail of the changes.
  - However mere presence of SPLMS does not guarantee program integrity.
  - Following control techniques are used to secure SPLMS:
    1. *Password Control:* every financially significant program stored in the SPL should be assigned a separate password.
    2. *Separation of Test Libraries:* here strict separation is maintained between production programs that are subject to maintenance in the SPL and those being developed. This is achieved by creating separate password controlled library for each programmer.

3. Audit Trail and Management Report

- SPL management software facilitates creation of reports that enhance management control and audit.
- *Program Modification Reports* describe in detail all program changes to each module and can be used to provide an audit trail of program changes over the life of the application. They can also be used to verify only the required changes are made to the program.

4. Program Version Number

- SPLMS assigns an automatic version number to each program stored in the SPL.
- On implementation they are assigned a version number of zero and with each modification the version number is increased by one.
- An unauthorized change is signaled by a version number on the production load module that cannot be reconciled to the number of authorized changes.

5. Controlling Access to Maintenance Commands

- Powerful maintenance commands are available for most library systems that can be used to alter or eliminate passwords, alter program version number etc.
- If not controlled, maintenance commands open the possibility of unrecorded and unauthorized program modification.
- Hence access to the maintenance commands themselves should be password controlled.

6. **Message Sequence Numbering**
    - An intruder in the communication channel may attempt to delete a message from a stream of messages, change the order of messages or duplicate a message.
    - Through message sequence numbering a sequence number is inserted in each message and any change to change the order will become apparent at the receiving end.

COMPUTER CENTRE SECURITY AND CONTROL

- Breach of computer security can be accidental or incidental.
- Both can lead to modification, destruction or disclosure of data and information.
- Hence there is a great need to ensure the security of computer system. Proper safeguards should be devised to prevent accidental data loss.
- The security administrator is responsible for balancing the benefits and costs of the various security measures.
- **Physical Security Measures**
    1. ***Fire Damage***
        - Fire is one of the major threats to physical security of a computer installation.
        - Some of the major ***features*** of a well designed fire protection system are:
            1. Strategically placed automatic and manual fire alarms
            2. Electronic fire detection system and extinguishing systems. Micro processor controlled fire detection can be designed and programmed to detect fire threats and activate necessary fire extinguishing systems like sprinklers and halogen gas. They can also be programmed to shut down the computer system in the event of fire.
            3. Manual fire extinguishers
            4. A control panel which shows where in the installation the alarm was triggered.
            5. Master switches for power and automatic extinguishing system.
            6. Building may be constructed from fire resistant materials.
            7. Clearly marked fire exits.
            8. When an automatic alarm is sent, signal should be transmitted to a permanently manned station.
            9. The security officer should arrange regular inspection of such systems.
            10. Staff training.

2. ***Water Damage***
   - Water damage may be caused by the fire, cyclones etc.
   - Some of the major ***features*** of a water damage protection system are:
     1. Water proof ceilings, walls and floors
     2. Adequate draining system
     3. Alarms
     4. In flood areas the installation should be constructed above high water level.
     5. Master switch for all water mains
     6. Dry pipe automatic sprinkler system that is charged by an alarm and activated by fire.
     7. Cover hardware by protective fabric when not in use.
3. ***Energy Variations***
   - Energy fluctuations may include Increases in power, decreases in power or loss of power.
   - Circuit breakers and battery backups can be used to protect against such risks.
4. ***Pollution Damage***
   - The major pollutant is dust. Computer installations should be made in a dust free environment.
   - Regular cleaning of ceilings, walls floors storage cabinets etc should be done.
5. ***Unauthorized Intrusion***
   - Physical intrusion may be physical intrusion of the site or eavesdropping (breaching privacy of data) on the installation by wire tapping, electronic bugs etc.
   - Alarms can be used to detect such bugs.

- **Disaster Recovery Plan (DRP)**
  - It involves contingency measures that the organization have adopted at key computing sites to recover from or to prevent any monumentally bad event or disaster.
  - Disaster may the result of:
    a. Natural causes, or
    b. Other sources. E.g. violent takeover, willful or accidental destruction of equipment.
  - The primary objective of a DRP is to assure the management that normality would be restored in a set time after any disaster thereby minimizing the losses.
  - ***General Components of a DRP***
    1. Emergency plan
       - It outlines the actions to be undertaken and the personnel to be notified immediately after a disaster occurs.

- It provides guidelines for shutting down equipment, power supply, removal of storage devices etc.
- It sets out evacuation procedures (for personnel)
- It provides return procedures to be followed as soon as the primary location is ready for operation.

2. Recovery Plan

- Recovery plan sets out how the full capabilities will be restored.
- *Steps Taken Under This Plan*
  - *i.* An inventory of all resources (hardware and software) should be taken.
  - *ii.* Criticality of applications and importance of their loss should be evaluated.
  - *iii.* An application systems hierarchy must be spelt out.
  - *iv.* Selection of a disaster recovery site must be made.
  - *v.* A formal backup agreement with another company must be made.

3. Backup Plan

- Organizations are always vulnerable to disasters. Therefore effective safeguards should be taken to have backup of anything that could be destroyed i.e. hardware and software.
- *Hardware Backup* - Stand by equipments
- *Software Backup* – Copies of existing applications, data files etc at another location.
- The backup copies of must be kept in a place which is not susceptible to the same hazards as the originals.

4. Test Plan

- It identifies deficiencies in the emergency, backup or recovery plan.
- It contains following *procedures* for conducting DRP testing.
  - *i.* Paper walk through (critical personnel in the plan's execution reasoning out what might happen in the event of different disasters)
  - *ii.* Localized tests (simulating system crash)
  - *iii.* Full Operational test (full simulation of system crash)

- **Disaster Recovery And Reconstruction** includes
  - Retrieving critical data and programs from offsite storage.
  - Installing and testing system software and application
  - Operating from off-site
  - Rerouting network communication traffic
  - Reconstruction of databases
  - Maintaining supply of necessary office goods.

- **DRP Testing**

  It involves:

  - Verification of the completeness or precision of DRP information.
  - Evaluation of the performance of personnel, and
  - Evaluation of the coordination between contingency team and external vendors.

  The test execution includes post-test which is a clean-up of activities like returning al resources to their proper places, deleting information from 3rd party systems etc.

- **Insurance**
  - Some residual risks always remain which cannot be covered by a DRP.
  - Such risks can be covered by transferring them contractually to a 3rd party by way of insurance.
  - Management must be careful to ensure that they consider all major potential losses are covered.
  - ***Types of Insurance Policies***
    1. Data processing policy
    2. Valuable papers and records policy
    3. Business interruption policy
    4. Extra expense insurance
    5. Errors and omissions insurance

INTERNET AND INTRANET CONTROLS

- Communication subsystem is responsible for transmitting data among all other subsystems within a system or for transmitting data to or receiving from other system.
- There are 2 major *Exposures* in the communication subsystem:
  - Component Failure, and
  - Intrusion
- **Component Failure**
  - There are 3 components to a communication subsystem: Communication lines, hardware and software.
  - Due to component failure transmission between sender and receiver can be disrupted, destroyed or corrupted in the communication system and it may also result in loss of database.
- **Subversive Threats**
  - An intruder attempts to violate the integrity of some components in the subsystem.
    1. *Invasive Tap* (by installing it on communication line)
    2. *Inductive Tap* (monitoring electromagnetic transmissions

- Using subversive threats an intruder can:
  1. Insert a message into the message stream,
  2. Delete a message,
  3. Modify the contents of a message,
  4. Alter the order of the message,
  5. Duplicate message,
  6. Deny message service between a sender and receiver, or
  7. Establish spurious associations.

➢ **Controlling Risks from Subversive Threats**

1. Firewalls

- A firewall is a system that enforces access control between two networks. It insulates the intranet from outside intruders.
- To accomplish this object:
  a. All traffic must pass through the firewall
  b. Only authorized traffic is allowed to pass through the firewall
  c. Firewall must be immune to penetration from both outside and inside the organization.
- Firewalls can be used to authenticate an outside user of the network, verify his level of authority and then direct the user to the program, data or service requested.
- Firewalls can also be used to insulate portions of the organization's intranet from internal access.
- ***Types of Firewalls***
  a. *Network Level Firewalls*
     - It consists of screening router that examines the source and destination addresses that are attached to incoming message. The firewall accepts or denies access requests based on filtering rules that have been programmed into it.
     - It provides low cost and low security access control
     - Such firewalls are comparatively unsecure as they are designed to facilitate free flow of information.
     - Hackers can break these firewalls using IP Spoofing technique.
  b. *Application Level Firewalls*
     - It provides a high level of customizable network security.
     - These firewalls run security applications called *proxies* that permit routine services like e-mail to pass through firewall. It can perform sophisticated functions such as logging or user authentication for specific tasks.

2. ***Controlling Denial of Service***
   - ***Normal Procedure to Connect Through Internet***

     Step 1: Connecting server sends an initiation called *SYN* packet to receiving server.

     Step 2: The receiving server then acknowledges the request by returning a *SYN/ACK* packet.

     Step 3: The initiating server responds with an *ACD* packet.
   - ***Denial Of Service Attack***
     - The attacker transmits hundreds of *SYN* packets to the targeted receiver and never responds with an *ACD* packet to complete the three way handshake (connection).
     - As a result ports of the targeted server are clogged with incomplete communication requests that prevent legitimate transactions from being received or processed.
     - Attackers usually use IP Spoofing (programs that randomize the source address of the attacker) to prevent the target server's firewall from identifying the source of attack.
     - DOS can severely hamper an organization's ability to use internet to conduct commerce.
   - ***Ways to Limit Such Attacks***

     i. Internet sites with firewalls must engage in a policy of social responsibility, and

     ii. Using security software to scan ports for half open connections and close such connections if necessary.

2. ***Encryption***
   - The sender uses an encryption algorithm to convert the original message (clear text) into coded equivalent (cipher text). At the receiving end the cipher text is decoded/decrypted back into clear text.
   - The encryption algorithm uses a key which is a binary number typically 56 to 128 bits in length. The more bits in the key, the stronger the encryption.
   - ***Approaches to Encryption***

     1. *Private Key Encryption*
        - It uses a single key known both to the sender and receiver to encrypt and decrypt the message.
        - The more individuals who need to know the key, the greater the probability of it falling to the wrong hands.
        - Example: DES (Data Encryption Standard)

2. *Public Key Encryption*
   - It uses 2 different keys: a public key to encrypt and private key to decrypt.
   - Each recipient has a unique private key which he uses to decrypt messages encrypted using a public key.
   - Here the private key need not be published and the same is retained by the recipient.

2. Message Transaction Log

- All incoming & outgoing messages and attempted access are recorded in a message transaction log.
- It can be used to prevent an intruder penetrating the system by trying different user IDs and passwords.

3. Call back Devices

- A call back devise require the dial –in user to enter a user ID and password. The system then breaks the connection and verifies the ID. If the caller is authorized, the device calls back the user and a connection is established.
- It limits access to authorized terminals or telephone numbers preventing an intruder penetrating the system.

PERSONAL COMPUTER CONTROLS

- The capabilities, adaptability and user friendliness of PCs are posing a serious challenge to the organization.
- **Security Risks Arising From the Use of PCs**
  - PCs are likely to be shifted from one place to another.
  - Decentralized purchase of PCs may result in hardware / software incompatibility.
  - Floppies can be used to transfer data.
  - Data security provided is poor.
  - Applications may not be thoroughly tested.
  - Segregation of duties is not possible.
  - The operating staff may not be adequately trained.
  - Risk of Viruses.
- **Security Measures That Could be Exercised**
  - Physically locking the keyboard.
  - Logging of equipment shifting.
  - Centrally coordinated PC purchases.
  - Floppies must be stored in secured places.
  - Data and programs on hard disks must be secured.

- Proper training programs to staff.
- Use Virus prevention and detection software.
- PCs and connected peripherals should be maintained regularly.

➢ **Weak Access Control**

- An intruder, to bypass the normal log on procedure of the OS, may try to force the computer to boot from another location (e.g. floppy drive). If he is successful he can load an uncontrolled OS to the memory and thus gets uncontrolled access to the data and programs stored in the hard disk of the system.
- ***Preventive Measures: Disk Locks***
  - Disk Lock is a devise that prevent unauthorized individuals from accessing the floppy drive of a computer.
  - *Memory Resident Disk Lock:* it's a program that prevents the computer from being booted from floppy drive. It may be password controlled so that it can be disabled if needed by an authorized user.
  - *Physical Disk Lock*: this devise fits into the floppy drive like a floppy disk to prevent its use and is secured with a physical lock and key.

➢ **Multilevel Password Control**

- This technique uses stored authorization tables to limit an individual's access to read only, data input, modification and data deletion capability in a shared computer system.

➢ **Inadequate Backup Procedures**

- The responsibility of providing backup in the PC environment is on the user and often because of lack of training and experience users may fail to do so.
- Disk failure is the primary cause of significant data loss in the PC environment. However there are a number of options to deal with this problem.
  1. Floppy Disk Backup
  2. Dual Internal Hard Disks
  3. External Hard Drives
  4. Tape Backup Devices
- A program can be configured to take backups automatically at regular intervals.

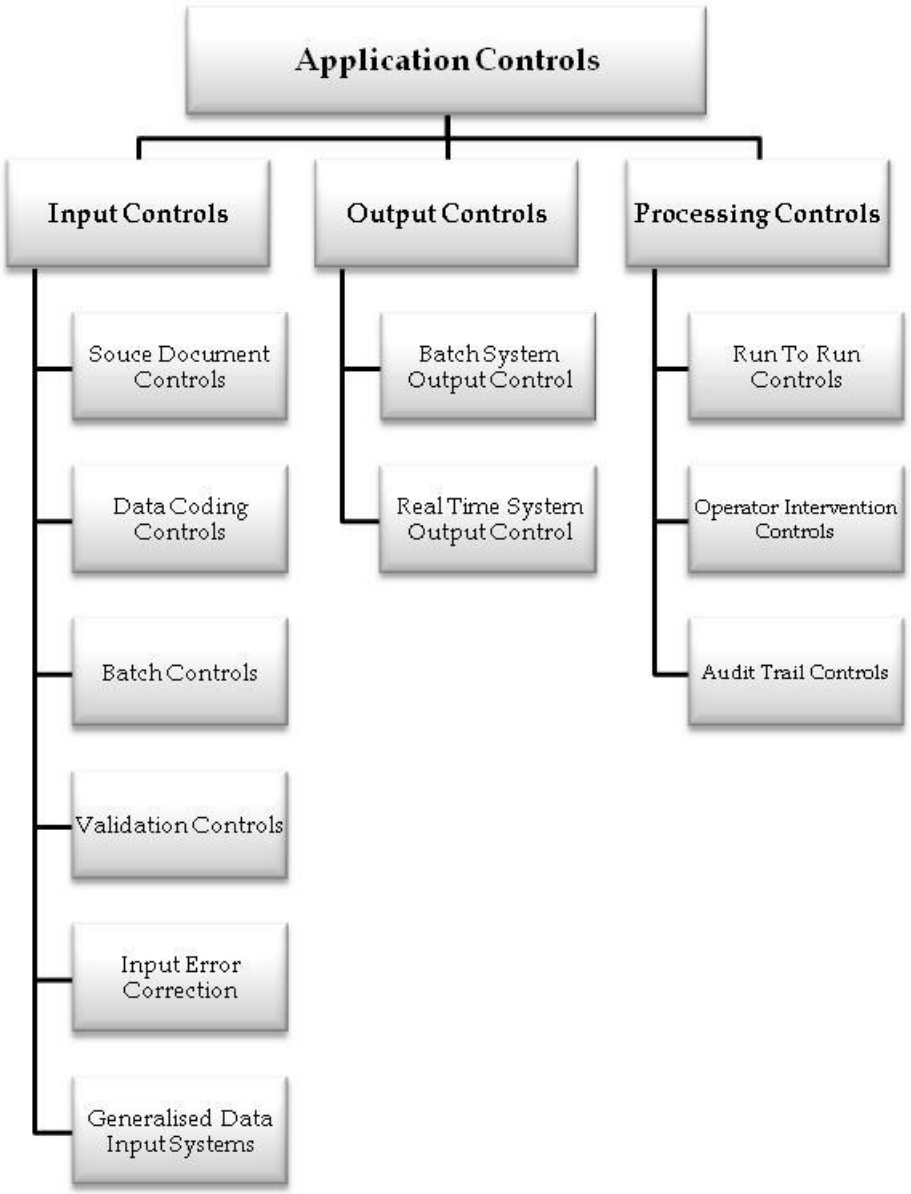
**

CHAPTER 14

CONTROLS IN EDP SET-UP: APPLICATION CONTROLS

APPLICATION CONTROLS

- Application controls deal with exposures within specific applications like payroll, purchases etc.
- Application controls fall into 3 categories: Input controls, Output controls and Processing Controls.



INPUT CONTROLS

- Input controls ensure that the data fed into the system by data collection component are valid, accurate and complete.
- Data input procedures can either be:
  - Source document triggered (batch), or
  - Direct Input (Real time)
- **Input Controls**
  1. ***Source Document Controls***
     - Such are controls are of prime importance in organizations where physical documents are used to initiate transactions.
     - Source document fraud can be used to remove assets from the organization.
     - Example: Fake Purchase order can be created to enter purchases in the name of a nonexistent vendor.
     - *Control Procedures*
       - **a.** Use of Pre-numbered source documents
       - **b.** Use source documents in a sequence and restricting access to such documents.
       - **c.** Periodical audit of source documents to find out missing documents.
  2. ***Data Coding Controls***
     - Coding controls are checks on the integrity of data codes used in processing.
     - *Types of Errors*
       - ***a.*** Transcription Errors
         - ***i.*** *Addition errors*: extra character is added to the code
         - ***ii.*** *Truncation errors*: a character is removed from the code
         - ***iii.*** *Substitution errors*: a character is replace by another one
       - ***b.*** Transposition Errors
         - ***i.*** *Single Transposition errors:* two adjacent characters are reversed
         - ***ii.*** *Multiple Transposition errors:* nonadjacent characters are transposed.
     - *Preventive Measure: Check Digits*
       - A check digit is a control digit(s) added to the code when it is originally assigned that allows the integrity of the code to be established during subsequent processing.
       - The check digit can be located anywhere in the code.
       - One of the most commonly used method is *11- Module Check digit*

2. ***Batch Controls***
   - Batch controls are an effective method of managing high volumes of transaction data through a system.
   - The objective of a batch control system is to reconcile the output produced with the input originally entered into the system.
   - It provides that:
     - All records in the batch are processed,
     - N records are processed more than once, and
     - An audit trail of transactions is created
   - To achieve these objectives, similar types of transactions should be grouped together in bathes and controlled throughout the data processing.
   - *Documents Used in Batch Control*
     - ***i.*** Batch Transmittal Sheet which contains all relevant details about the batch like batch number, number of records, hash total, control total etc. it's prepared by the used dept and submitted to data control along with source documents.
     - ***ii.*** Batch Control Log which contains relevant details of batch before processing and after processing and is maintained by the data control clerk.
   - *Hash Total:* It's a simple technique that uses non financial data to keep track of the records in a batch. E.g. total of purchase order numbers / inventory items number etc.

2. ***Validation Controls***
   - Validation controls are intended to detect errors in transaction data before the data are processed.
   - These controls are most effective when performed as close to the source of the transaction as possible.
   - Some validation procedures are performed by each processing module prior to updating the master file record.
   - *Levels of Validation Controls*
     - ***i.*** Filed Interrogation *(programmed procedures that examine the characters of the data in the field)*
       1. *Limit Checks:* the field is checked by the program to ensure that its value lies within certain predefined limits.
       2. *Picture Checks:* these check whether incorrect characters are entered
       3. *Valid Code Checks:* checks are made against predetermined transactions codes, tables or order data to ensure that input data are valid. Such codes or tables may either be embedded in the program or stored in a different file.

4. *Check Digit*
5. *Arithmetic Checks:* arithmetic is performed in different ways to validate the result of other computations of the values of selected data fields.
6. *Cross Checks:* are employed to verify fields appearing in different files to see that the result tally.

ii. Record Interrogation

1. *Sequence Checks:* to detect any missing transaction
2. *Format Completeness Checks:* to check the presence and position of all fields in a transaction
3. *Redundant Data Checks:* used in sequential processing to find duplicates
4. *Combination Checks:* to check for invalid combinations like credit to individuals
5. *Passwords to various users*
6. *Access Privilege Checks*

iii. File Interrogation *(to ensure that correct file is being processed by the system)*

1. *Internal Label Checks:* verity that the file processed is one the program is calling for using an external tag placed on the file. The OS generally creates the internal label. The system matches the file name and serial number in the header label with the programs file requirements.
2. *Version Checks:* verify the version of the file being processed is correct.
3. *An Expiration Date Check:* verify the expiration date before deleting a file to ensure that only those files that have been expired are deleted.

3. Input Error Correction

- It refers to a controlled process to ensure that errors detected are dealt with completely and correctly.
- *Error Handling Techniques*
  - ***i.*** *Immediate Correction*
    - If direct data validation systems are used, error detection and correction can be done simultaneously.
  - ***ii.*** *Creating Error File*
    - In batch systems individual errors are flagged to prevent processing and at the end of validation procedure, these flagged

records are removed from the batch and are placed in a temporary error holding file.

- At each validation point the system automatically adjusts the batch control totals and hash totals to reflect the removal of error records from the batch.
- Simultaneously an authorized person will make corrections to the error records and resubmit them as a separate batch for reprocessing.
- Errors detected during processing require careful handling as records may be partially processed.
- There are 2 methods for dealing with such complexity:
  - *I.* Reverse the effects of partial processing, or
  - *II.* Reinsert corrected records to the processing stage in which the error was detected.

iii. *Rejecting Entire Batch*

- Some forms of errors are associated with the entire batch and are not attributable to individual records. E.g. mismatch in batch control totals.
- The solution is to cease processing and return the batch to data control to evaluate, correct and resubmit.

PROCESSING CONTROLS

1. **Run To Run Controls**
   - They use batch figures to monitor the batch as it moves from one programmed run to another.
   - Theses controls ensure that each run in the system processes the batch correctly and completely.
   - ***Uses of Run to Run Controls***
     - ***i.*** Recalculating control totals (hash totals, record counts etc) after each run and comparing to corresponding values in the control records.
     - ***ii.*** Comparing the transaction code of each record with transaction code in the control record.
     - ***iii.*** Comparing the sequence of each record in the batch with the previous record to ensure that proper sorting took place (Sequence Checks).

2. **Operator Intervention Controls**
   - Systems require operator intervention sometimes to initiate certain actions. Such intervention increases the potential for error (human error).
   - Operator intervention controls are used to limit such intervention.
   - Parameter values and program start points should to the extent possible be derived logically or provided to the system through look-up tables.
3. **Audit Trail Controls**
   - The preservation of an audit trail is an important objective of the process control. Following techniques are used to preserve audit trails in a CBIS:
     - ***i.*** *Transaction Logs:* Every successfully processed transaction is recorded in a transaction log. It serves as a journal. There are *Two Reasons* for creating a transaction log:
       - ***a.*** It's a permanent record f transactions, and
       - ***b.*** Not all the records in the validated transaction file may be successfully processed.

       Unsuccessful transactions are placed in an error file.
     - ***ii.*** *Transaction Listings:* it's a hard copy transaction listing of all successful transactions.
     - ***iii.*** *Log of Automatic Transactions:* all internally generated automatic transactions should be recorded in transaction log.
     - ***iv.*** *Listings of Automatic Transactions:* it's a listing of all internally generated transactions.
     - ***v.*** *Unique Transaction Identifiers:* each transaction processed by the system is uniquely identified with a transaction number and this number helps to trace a particular transaction through the database.
     - ***vi.*** *Error Listings:* it's a listing of all records.

OUTPUT CONTROLS

- Output controls ensure that system output is not lost, misdirected or corrupted and that privacy is not violated.
- The choice of controls employed to protect system output is influenced by the type of processing method in use.
- Various out exposures and controls are discussed below.

1. **Controlling Batch System Output**
   - ***a. Tape and Disk Output Control***
     - Special care must be taken to ensure accuracy in encoding of information on magnetic tapes and disks as the same is not verified manually.

- Hardware controls such as parity bit checking and software controls such as check digits can be used to ensure accuracy.
- Disk drives and tape drives have built in dual recording mode to enable these machines to check on recording accuracy. It's called *Echo Check.* When the disk is encoded with information the same is read and compared to original output. On confirmation of identical result the disk drive signals the processor that writing operation was successful.
- Labels can be used as control mechanism.

b. Printed Output Control

i. *Verification of Output*

- Verification controls are governed by the relationship which the output bears to the input and the processing that created it. They are of three types:

1. Output directly related to input

- Output that is identical with input, which usually results from updating or creating a file and tasks the form of lists or documents.
- Output that is in part identical with input but includes additional information usually involving standing data.

*2.*Output indirectly related to input

- It include output generated by the programs on the basis of:
  - Current input data,
  - Previous or latest input data
  - All input for a given period.

*3.*Exception reports

- These reports include items identified by the computer programs from a scrutiny of input data or master files as not satisfying conditions specified in the program.
- Their complete and accurate production almost always depends on the correct functioning of the computer programs.

ii. *Distribution of Output*

- If the verification is carried out in the computer dept or the output is not verified with the controls established over input or master file procedures are required to ensure that the user dept responsible receives all output intact.

iii. *Procedures For Acting on Exception Records*

- Exception reports provide the information on which important control functions are based.
- An independent review of exception records is carried out to ensure that exceptional items are promptly investigated and acted upon.

2. <u>Controlling Real Time Systems Output</u>

- The primary threat to a real time output is the interception, disruption, destruction or corruption of the output message as it passes along the communication link.
- Threats come from 2 types of exposures:
  i. Equipment failure, and
  ii. Subversive acts.

**

CHAPTER 15

DETECTION OF COMPUTER FRAUDS

INTRODUCTION

- Fraud refers to any and all means a person uses to gain an unfair advantage over another person. It can be committed by someone within the organization or by an external party.
- Since employees understand company's system and its weaknesses, they are better able to commit fraud, evade detection and cover their tracks.
- Fraud perpetrators are often referred to as ***white Color Criminals.***

COMPUTER FRAUDS

- ***Definition*** **:** "Using a computer to cause prejudice, in the case of financial and/or reputational damage, to a business"
- Computer fraud *includes* (but not limited to):
    1. Clearly recognizable frauds such as investment frauds.
    2. Hacking i.e. unauthorized access and unauthorized modification to computers or web pages.
    3. Manipulation of computer system to obtain money from an employer or a third party e.g. diversion of payments by creating false vendors etc.
    4. Theft and/or destruction of confidential and sensitive information.
    5. Abuse of computer systems by employees i.e. using the computer systems by employees for personal purposes.
    6. Software piracy i.e. using counterfeit or unlicensed software.
    7. Use or the conspiracy to use computer resources to commit an offence.

REASONS FOR INCREASING PROBABILITY FOR COMPUTER FRAUDS

1. Businesses are dependent on standalone computers or networks.
2. Individual businesses are linked through computer networks.
3. Growth of e-commerce.
4. Growth of e-cash.

COMPUTER FRAUD VS CONVENTIONAL FRAUD

1. Computer fraud is easily hidden and hard to detect than conventional fraud.
2. Evidence of a computer fraud is hard to find and also difficult to present to a court in an effective or legally admissible way.
3. It can be easily committed in ways that may not be obvious.

RISKS TO BUSINESS FROM COMPUTER FRAUDS

1. **Internal Threats**
   - Internal fraud is a greater risk to business than external fraud.
   - ***Types of Internal Fraud***
     - *i. Input*
       - The simplest way to commit fraud is to alter computer input.
       - *Collusive fraud:* using documents to divert payments
       - *Disbursement fraud:* the fraudster causes the company to pay more or pay for good never delivered.
       - *Payroll fraud:* enter data to increase salary
       - *Cash receipt fraud:* hides theft by falsifying system input.
     - *ii. Processor*
       - Committed through unauthorized system use. It includes theft of computer time and services. E.g. Goofing: Surfing the net for personal entertainment on company time)
     - *iii. Computer Instructions*
       - It involves tampering with (modifying the software, making illegal copies or using it in an unauthorized manner) the software that processes the data.
       - In order to commit such frauds, specialized knowledge about computer programming is necessary.
     - *iv. Data*
       - It's undertaken by altering or damaging a company's data files or by copying, using or searching them without authorization. Data can also be stolen, destroyed, changed or defaced.
     - *v. Output*
       - It involves stealing or misusing system output.
     - *vi. Malicious Alterations of Email*

2. **External Threats**
    - Removal of information
    - Destruction of system integrity
    - Interference with web pages
    - Transmission of viruses
    - Interception of email and electronic payments.

REASONS FOR INCREASE IN INTERNET FRAUDS

1. Internet is unregulated in the sense that anyone can start a website as there is no central authority to verify the validity.
2. A web site can be setup anywhere in the world at very low cost and can reach anywhere else in the world.
3. There is no easy way to separate the genuine from the false.
4. A web site claiming spurious credibility may cause otherwise prudent individuals to become involved in fraudulent activities.
5. A web site may operate outside the legal jurisdiction of the country in which the victim of the fraud resides.

RISE IN COMPUTER FRAUDS: CAUSES

- Due to the following reasons it's very difficult to know for sure how many companies are subjected to fraud.
    1. Ambiguity in defining what constitutes computer fraud. E.g. software piracy is not considered by many as fraud.
    2. Many computer frauds go undetected.
    3. Many frauds discovered are not reported.
    4. Most networks have a low level of security
    5. Many web sites give step by step instructions on how to perpetrate computer frauds and abuses.
    6. Low enforcement is unable to keep up with growing number of cases.

COMPUTER FRAUD AND ABUSE TECHNIQUES

Sl No	Technique	Description
1	Cracking	Unauthorized access to and use of computer systems. Crackers are hackers with malicious intends.
2	Hacking	Unauthorized access to and use of computer systems. Unlike hackers crackers don't intend to cause any damages.
3	Data Diddling	Change data before, during or after it's entered into the system in order to delete, alter or add key system data.
4	Data Leakage	Unauthorized copying of company data
5	Denial of Service Attack	Attacker sends several emails from random IP addresses to clog up target server.
6	Eavesdropping	Listening to private voice or data transmissions
7	E mail forgery	Sending an email that
8	E mail threats	Sending threatening mails to try and get recipient to do something that would make it possible to defraud him.
9	Internet misinformation	Using the net to spread false or misleading information about companies.
10	Internet terrorism	Using the net to disrupt e commerce and to destroy company and individual communications
11	Logic time bomb	Program that lies idle until some specified circumstance or particular time triggers it. Once triggered it sabotages the system by destroying programs.
12	Impersonation	Gaining access to a system by pretending to be an authorized user.
13	Password cracking	Stealing passwords and using them to gain access to system
14	Piggybacking	Tapping into a telecommunication line and latching on to a legitimate user before he logs on to the system.
15	Round-down	Computer rounds down all calculations to two decimal points and the remaining fraction are placed into perpetrator's account.
16	Salami technique	Tiny slices of money are stolen over a period of time by increasing the expenses by a tiny percentage and pocketing this difference.
17	Scavenging	Gaining access to confidential information by searching corporate records.
18	Social engineering	Perpetrator tricks an employee into giving out the information needed to get into the system.
19	Software piracy	Copying computer software without publisher's permission.
20	Spamming	E mailing the same message to everyone on one or more individuals or user groups.

Sl No	Technique	Description
21	Super zapping	Unauthorized use of special system programs to bypass regular system controls and perform illegal acts.
22	Trap door	Perpetrator enters the system using a back door that bypass normal system controls and perpetrates fraud.
23	Trojan horse	Unauthorized computer instruction in an authorized and properly functioning program.
24	Virus	Segment of executable code that attaches itself to software, replicates itself and spreads to other systems or files. It causes damage to system resources.
25	War dialing	Programming a computer to search for an idle modem by dialing thousands of phone lines. If it captures an idle modem it gains access to the computer connected to that modem and through that computer access to connected network is obtained.
26	Worm	Similar to a virus except that it's a program rather than a code segment hidden in a host program.

PREVENTING COMPUTER FRAUDS

1. Make fraud less likely to occur by taking steps to increase employee integrity and reduce likelihood of commission of fraud by employees.
2. Use proper hiring and firing practices so that dismissed employees are removed from sensitive jobs immediately and denied access to the computer system.
3. Manage disgruntled employees.
4. Train employee in security and fraud prevention measures.
   Employees should be trained in the following areas:
   - ***i.*** Security measures
   - ***ii.*** Telephone disclosures (nothing should be disclosed until the identity is confirmed)
   - ***iii.*** Fraud awareness (made aware of fraud, it prevalence and dangers)
   - ***iv.*** Ethical considerations. Ethical standards should be promoted.
   - ***v.*** Punishment for unethical behavior
   - ***vi.*** Educating employees
   - ***vii.*** Manage and track software licenses
   - ***viii.*** Require signed confidentiality agreements.

INCREASING DIFFICULTY TO COMMIT FRAUD

1. Develop a strong system of internal controls.
2. Segregate duties
3. Require vacations and rotation of duties to prevent ongoing frauds
4. Restrict access to computer equipment and data files
5. Encrypt data and program
6. Protect telephone lines. (Phreaker: computer hacker who attacks telephone system)
7. Protect the system from viruses by using antivirus software which can scan the system for virus strains (specific characteristics of a virus)
8. Control sensitive data
9. Control laptops by:
    - **a.** Establishing laptop security policies
    - **b.** Password protecting and encrypting data on the hard drive
    - **c.** Not storing confidential information on hard drives of laptop.

IMPROVING DETECTION METHODS

1. Conduct frequent audits: external and internal audits as well as special network security audits.
2. Use a computer security officer to monitor the system and disseminate information about improper system uses and their consequences.
3. Use computer consultants to test and evaluate the security procedures.
4. Monitor system activities and record in a log.
5. Use of fraud detection software to search for fraud symptoms like patterns left by intruders.

REDUCE FRAUD LOSSES

To minimize fraud losses, these methods can be followed:

1. Maintain adequate insurance
2. Keep backup of all programs and data
3. Develop contingency plan for dealing with fraud
4. Use software to monitor system activity.

DETECTION OF COMPUTER FRAUDS: DISK IMAGING AND ANALYSIS TECHNIQUES

- It enables the fraud investigator to discover evidence of transactions that the fraudster thought were inaccessible or had been destroyed.
- Such techniques can be used where evidence of commission of fraud is retained in a computer. e.g. forged email etc
- The technique can equally be applied to a network or any other storage media.
- Stages are as follows:
    1. By attaching an imaging hardware to the parallel port of the computer and running the imaging software, an exact copy of the computer hard drive can be taken leaving the original intact.
    2. The image copy of the disk is processed and areas of storage containing partially overwritten files and files which have been marked as deleted but not overwritten are recovered (when a file is deleted, only the reference point to that file created in the file allocation table at the time of creation of file is removed. The file itself is not deleted).
    3. The final stage is the analysis of the processed image. This is done by search software which can be programmed to find references to suspect transactions.
- Information can be recovered for investigation from:
    1. Free space (may contain deleted but not overwritten files)
    2. Lost chains (areas in the disk without a name or disconnected from the file system)
    3. Slack space (unused areas disk space allocated to files in allocation blocks i.e. of the thousands of bytes allocated some bytes may remain unused and these may contains parts of deleted files)
    4. Deleted files i.e. files in trash bin
    5. Windows SWAP file. SWAP is a disk cache created by the OS and it may contain entire documents, memoranda and database information.
    6. Internet cache file or temporary internet files. Web pages accessed are stored by windows in a temporary folder called "temporary internet files".
       Note: users don't generally check on such SWAP and temporary files as these are hidden from the user.

**

CHAPTER 16

CYBER LAWS AND INFORMATION TECHNOLOGY ACT, 2000

OBJECTIVES AND SCOPE OF THE INFORMATION TECHNOLOGY ACT, 2000

➔ **Objectives**

a. to grant legal recognition for transactions carried out by means of electronic communication (e commerce) in place of paper based methods of communication,
b. to give legal recognition to digital signature for authentication of any information
c. to facilitate e-filing of documents with government departments
d. to facilitate electronic storage of data
e. to facilitate and give legal sanctions to EFT between banks and financial institutions
f. to give legal recognition for keeping books of accounts by bankers in e-form
g. to amend
    - Indian Penal Code,
    - Indian Evidence Act, 1872
    - The Banker's Book Evidence Act,1891 and
    - The RBI Act, 1934.

➔ **Scope**

- The act shall extend to the whole of India.
- It applies to any offence or contravention there under committed outside India by any persons unless otherwise provided in the act.
- It shall come into force on such date as the Central Government may prescribe.

➔ **Exceptions**

The act shall not apply to the following:

1. A negotiable instrument as defined in Sec 13 of Negotiable Instruments Act, 1881
2. A power-of-attorney as defined in Sec 1A of Power of Attorney Act, 1882
3. A trust as defined in Sec 3 of Indian Trusts Act, 1882
4. A will as defined in Sec 2(h) of Indian Succession Act, 1925
5. Any contract for the sale or conveyance of immovable property or any interest in such property
6. Any such class of documents or transactions as may be notified by the Central Government in the official Gazette.

DEFINITIONS (SECTION 2)

- **Sec 2(d): Affixing Digital Signature**

  With its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of a digital signature.

- **Sec 2(f): Asymmetric Crypto System**

  System of a secure key pair consisting of a private key for creating a digital signature and public key to verify the digital signature.

- **Sec 2(i): Computer**

  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.

- **Sec 2(j): Computer Network**

  The interconnection of one or more computers through—

  i. The use of satellite, microwave, terrestrial line or other communication media, and
  ii. Terminals or a complex consisting of two or more interconnected computers whether or not interconnection is continuously maintained.

- **Sec 2(k): Computer Resource**

  Computer, computer system, computer network, data, computer database or software.

- **Sec 2(p): Digital Signature**

  Authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of Section 3.

- **Sec 2(t): Electronic Record**

  Means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.

- **Sec 2(v): Information**

  Includes data, text, images, sound, voice, codes, computer programs, software and databases or micro film or computer generated micro fiche.

- **Sec 2(za): Originator**

  A person, who sends, generates stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary.

- **Sec 2(zc): Private Key**

  The key of a key pair used to create a digital signature.

- **Sec 2(zd): Public Key**

  The key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate.

- **Sec 2(ze): Secure System**

  Computer hardware, software and procedure that –

  a. Are reasonably secure from unauthorized access and misuse,
  b. Provide a reasonable level of reliability and correct operation
  c. Are reasonably suited to performing the intended functions, and
  d. Adhere to generally accepted security procedures.

- **Sec 2(zh): Verify**

  In relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether –

  a. The initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber
  b. The initial electronic record is retained intact or has been altered since such electronic record was so affixed with digital signature.

AUTHENTICATION OF ELECTRONIC RECORDS USING DIGITAL SIGNATURES

(CHAPTER II – SECTION 3) ★★★★★

➔ This section provides conditions subject to which an electronic record may be authenticated by means of affixing digital signature.

➔ **Creation of Digital Signature**

Step 1: The electronic record is converted into a *message digest* by using a mathematical function known as *'hash function'* which digitally freezes the electronic record thus ensuring the integrity of the content of intended communication contained in the electronic record.

Step 2: The identity of the person affixing the digital signature is authenticated through the use of a private key which attaches itself to the message digest and which can be verified by anybody who has the public key corresponding to the private key.

➔ **Hash Function**

It's an algorithm mapping or translation of one sequence of bits into another smaller set known as *"hash result"* such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as it's input making it computationally infeasible—

a. To derive or reconstruct the original electronic record from the hash result produced by the algorithm,
b. That two electronic records can produce the same hash result using the algorithm

ELECTRONIC GOVERNANCE

(CHAPTER III – SECTIONS 4 TO 10)

Section 4: Legal recognition of electronic records

Section 5: Legal recognition of digital signature.

Section 6: It lays down the foundation of e-governance. It provides that

i. The filing of any form, application, or other documents,
ii. Creation, retention or preservation of records,
iii. Issue or grant of any license or permit, receipt or payment in government offices and it's agencies

May be done through the means of electronic form

Section 7: Retention of records in electronic form

Section 8: Publication of rules, regulations and notifications in the Electronic Gazette.

Section 9: it provides that the conditions stipulated in Sections 6, 7 and 8 shall not confer any right to insist that the document should be accepted in an electronic form by any Ministry or department of the Central or State Government.

Section 10: ***Power of Central Government to make Rules in respect of Digital Signatures***

The Central Government may prescribe by rules the following:

1. The type of digital signature
2. The manner and format in which the digital signature shall be affixed
3. The manner or procedure which facilitates identification of the person affixing the digital signature
4. Control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments, and
5. Any other matter which is necessary to give legal effect to digital signatures.

ATTRIBUTION, RECEIPT AND DISPATCH OF ELECTRONIC RECORDS

(CHAPTER IV – SECTIONS 11, 12 AND 13)

Section 11: This section lays down the manner in which an electronic record is to be attributed to the person who originated it.

Section 12: It provides the manner in which acknowledgement of receipt of an electronic record by various modes is to be made.

Section 13: It provides for the manner in which the time and place of dispatch and receipt of an electronic record sent by the originator shall be identified.

Place of dispatch and Receipt: Principal place of business or usual place of residence or registered office of the originator or addressee as the case may be.

SECURE ELECTRONIC RECORDS AND SECURE DIGITAL SIGNATURES

(CHAPTER V – SECTIONS 14, 15 AND 16)

Section 14: Conditions to qualify electronic records and digital signature as being secure.

Section 15: It provides for the security procedure to be applied to digital signature for being treated as a secure digital signature.

Section 16: It provides for the power of the Central Government to prescribe the security procedure in respect of secure electronic records and secure digital signatures.

REGULATION OF CERTIFYING AUTHORITIES

(CHAPTER VI – SECTIONS 17 TO 34)

Section 17: Appointment of Controller and other officers to regulate Certifying Authorities.

Section 18: Functions which the Controller may perform in respect of activities of Certifying Authorities.

Section 19: Power of the Controller (with previous approval of the Central Government) to grant recognition to foreign Certifying Authorities.

Section 20: It provides that the Controller shall be acting as a repository of all Digital Signature Certificates issued under the Act. He shall ensure the secrecy and privacy of the digital signatures. He shall maintain a database of all public keys in such a manner that they are available to general public.

Section 21: It provides the form, fees and other documents needed to be submitted by a Certifying Authority to apply for the issue of the license to 'Issue DSC' by the Controller.

Section 22: it provides that the application as mentioned in Section 21 shall be accompanied by

a. A certification practice statement and
b. Statement including the procedure with respect to identification of the applicant.
c. Fees not exceeding Rs 25000.
d. Other documents as may be prescribed.

Section 23: The application for renewal of a license. (Fee not to exceed Rs 5000)

Section 24: The procedure for grant or rejection of license after giving the applicant a reasonable opportunity of being heard.

Section 25: It provides that the Controller may revoke a license, on the grounds such as incorrect or false material particulars being mentioned in the application, contravention of the provisions of the act, rules, regulation or order issued there under, after giving the applicant a reasonable opportunity of being heard.

No license shall be suspended for a period exceeding 10 days unless the Certifying Authority has been a given a chance to present his case.

Section 27: The Controller may in writing authorize the Deputy Controller, Assistant Controller or any other officer to exercise any of his powers under the act.

Other powers

The Controller shall have the power to investigate contravention of the provisions of the Act either by himself or through any officer authorized in this behalf.

Such person shall have access to any computer system, data or any other material connected with such system if he has reasonable cause to suspect that contravention of the provisions of the act or rules is being committed.

Section 30: ***Duties of Certifying Authorities***

1. Duties in respect of digital signatures
    - ***a.*** Make use of hardware, software and procedures that are secure from intrusion and misuse,
    - ***b.*** Provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions,
    - ***c.*** Adhere to security procedure to ensure that the secrecy and privacy of the digital signatures are assured, and
    - ***d.*** Observe such other standards as may be prescribed
2. Ensure that every person employed by him complies with provisions of this Ac and rules made there under.
3. Display its license at a conspicuous place of the office premises. Surrender the license to the Controller when the same is revoked or suspended.
4. Disclose its DSC which contains the public key corresponding to the private key used by that certifying Authority and other relevant facts ***(Section 34).***

DIGITAL SIGNATURE CERTIFICATION

(CHAPTER VII – SECTION 35 TO 40)

Section 35: The procedure for issuance of digital signature certificate (fee not more than Rs 25000)

Conditions

No DSC shall be granted unless the Certifying Authority is Satisfied that:

a. The applicant holds the private key corresponding to the public key to be listed in the DSC.
b. The applicant holds a private key, which is capable of creating a digital signature,
c. The public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant.

Suspension: No certificate shall be suspended for a period exceeding 15 days unless the subscriber has been given an opportunity of being heard.

Section 38: Revocation of DSC by publishing a notice of suspension or revocation of aDSC.

DUTIES OF SUBSCRIBERS

(CHAPTER VIII – SECTIONS 40, 41 AND 42)

1. On acceptance of the DSC the subscriber shall generate a key pair using a secure system.
2. The subscriber shall exercise all reasonable care to retain control of his private key corresponding to the public key.
3. If the private key has been compromised the subscriber must immediately communicate the fact to Certifying Authority.

PENALTIES AND ADJUDICATION

(CHAPTER IX – SECTIONS 43 TO 47)

Section 43: ***Penalty for Damage to Computer, Computer System or Network***

It deals with penalty for damage to computer, computer system or network by any of the following methods

i. Securing access to computer etc
ii. Downloading or extracting any data, computer database or information from such computer system or those stored in any removable storage medium.
iii. Introducing any computer containment or virus into the computer etc
iv. Damaging any computer etc, data, database or programs
v. Disrupting any computer or computer system
vi. Denying access to any person authorized to access the computer
vii. Providing assistance to any person to access any computer etc in contravention of any provisions of this act
viii. Charging the services availed by one person to the account of another person by tampering with or manipulating any computer etc.

Computer Virus means a representation of information, knowledge, 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 network and are intended for use in a computer, computer system or computer network.

Section 46: Power to adjudicate contravention under the act to an officer not below the rank of a Director to the Government of India or State Government.

Section 47: It provides that while deciding upon the quantum of compensation the adjudicating officer shall have due regard to the amount of gain or unfair advantage and the amount of loss caused to any person as well as the respective nature of the default.

CYBER REGULATIONS APPELLATE TRIBUNAL

(CHAPTER X – SECTIONS 48 TO 64)

Section 48: It provides for the establishment of one or more Appellate Tribunals to be known as Cyber Regulation Appellate Tribunal (CRAT).

- It shall consist of one person *only* called the Presiding Officer of the Tribunal and shall be appointed by the Central Government.
- The presiding officer shall be a person qualified to be a judge of high court or
- Has been a member of the Indian Legal Service in the post (Grade I) of that service for at least 3 years.
- He shall hold office for a term of 5 years or up to the maximum age of 65 whichever is earlier.

Section 52: It provides for the salary and allowances and other terms and conditions of service of the Presiding Officer.

Section 53: Provides that in the situation of any vacancy occurring in the office of the Presiding Officer, the Central Government shall appoint another person in accordance with the provisions of the Act.

Section 54: Resignation and removal of the Presiding Officer.

Appeal to CRAT

1. An appeal can be made by an aggrieved person against an order of the adjudicating officer to the CRAT.
2. The appeal must be made within 45 days of the receipt of the original order.
3. The Tribunal may accept the appeal after the expiry of 45 days if it is satisfied that there was sufficient cause for not filing it within the period.
4. No appeal shall be entertained if the original order was passed with the consent of both the parties.

Section 58: ***Powers and Procedure of the Appellate Tribunal***

- The tribunal shall have the powers of a Civil Court under the Code of Civil Procedure, 1908.
- It shall have following powers:
    i. Summoning and enforcing the attendance of any person and examining him on oath,
    ii. Requiring production of documents and other electronic records,
    iii. Receiving evidence on affidavits,
    iv. Reviewing its decisions,
    v. Issuing commissions for examination of witness etc.

Section 61: No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer has jurisdiction to determine

Section 62: Appeal to High Court on question of law or fact arising out of the order of the CRAT within 60 days from the receipt of the order.

Section 63: Any contravention under this Act may be compounded by the Controller or Adjudicating Officer either before or after the institution of adjudicating proceedings subject to such conditions as he may impose.

Exception: This provision shall not apply to a person who commits the same or similar contravention within a period of 3 years from the date on which the first contravention, committed by him, was compounded.

Section 64: Recovery of penalty as arrears of land revenue and suspension of the license or DSC till penalty is paid.

OFFENCES

(CHAPTER XI – SECTIONS 65 TO 78)

Section	Offence	Penalty
65	Tampering with computer source documents	a. Imprisonment up to 3 years, or b. Fine which may extend to Rs 2lakhs, or c. Both.
66	Hacking i.e. the act of destroying or deleting or altering any information residing in a computer resource or diminishing its value or utility, or affecting it injuriously in spite of knowing that such action is likely to cause wrongful loss or damage to public or to that person	
67	Publishing, transmitting or causes to publish or transmit any material which is obscene in electronic form	*First Conviction* a. Imprisonment up to 5 years, or b. Fine up to Rs 1 lakh *Subsequent Conviction* a. Imprisonment up to 10 years, or b. Fine up to Rs 2lakhs.
68	Failure to comply with an order issued by the Controller, directing to take such measures or cease carrying on such activities as specified, by Certifying Authority or any employee of such authority	a. Imprisonment up to 3 years, or b. Fine which may extend to Rs 2lakhs, or c. Both.

Section	Offence	Penalty
70	Unauthorized access to a computer, computer system or network declared by the Central Government as "Protected" vides a notification.	a. Imprisonment up to 10 years, or b. Fine.
71	Misrepresenting or suppressing any material fact from the Controller or Certifying Authority	a. Imprisonment up to 2 years, or b. Fine which may extend to Rs 1 lakh, or c. Both.
72	Breach of confidentiality and privacy of electronic records, books, information etc	
73	Publishing a DSC false in material particulars or otherwise making it available to any other person	
74	Knowingly publishing any DSC for fraudulent purposes	

Section 69: ***Power of Controller to Intercept Transmissions***

The controller, if satisfied that it is necessary or expedient so to do in the interest of

a. Sovereignty and integrity of India,
b. Security of the State,
c. Friendly relation with foreign states, or
d. Public order

Is empowered to intercept any information transmitted through any computer system or network.

Section 76: It provides for the confiscation of any computer, computer system, floppies, CDs, tape drives or any other accessories related thereto in respect of contravention of any provisions of the Act, rules and regulations.

Section 77: The penalty and confiscation provided under this Act shall n***ot*** interfere with other punishments provided under any other law for the time being in force.

Section 78: Power to investigate the offences under this Act by a police officer not below the rank of DSP.

NETWORK SERVICE PROVIDERS NOT TO BE LIABLE IN CERTAIN CASES

(CHAPTER XII – SECTION 79)

The network service providers (intermediary) shall not be liable to any third party information (information dealt with by such provider in the capacity of an intermediary) or data made available by him if he proves that the offence was committed without his knowledge or consent.

MISCELLANEOUS PROVISIONS

(CHAPTER XIII - SECTIONS 80 TO 89)

Section 80: ***Power of police officer and other officers to enter, search, arrest etc.***

i. Notwithstanding anything contained in Code of Criminal Procedure 1973,
   a. Any police officer not below the rank of DSP, or
   b. Any other officer of the Central or State Government, if so authorized by the Central Government,

   May enter any public place (includes public conveyance and any place accessible to public) and search and arrest ***without warrant*** any person found therein who is reasonably suspected of having committed or of committing or is about to commit any offence under this Act.
ii. Where any person is arrested by any person other than a police officer, such officer shall immediately send the arrested person to
   a. A magistrate having jurisdiction or
   b. The officer in charge of the nearest police station.

Section 85: ***Liability of Companies***

i. Where a company commits any offence under this Act , every person, who at the time of contravention, was in charge of and was responsible for the conduct of the business of the company shall be guilty of such contravention.
ii. *Exception:* Such person shall not be liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent the contravention.
iii. Where such contravention was committed with the connivance or consent of or due to negligence on the part of any director, manager, secretary or other officer of the company, such officer shall be deemed to be guilty and shall be liable to proceeded against and punished accordingly.
iv. Company includes a firm and AOP.

Section 87: ***Power of Central Government to make rules***

The Central Government is empowered to make rules in respect of following matters;

1. The manner in which any matter may be authenticated by a digital signature
2. The manner and format in which electronic records shall be filed or issued
3. The type of digital signature, manner and format in which It may be affixed
4. The security procedure for the purpose of creating same electronic record and secure digital signature.

5. The qualification, experience and terms and conditions of service of Controller, Deputy Controllers and Asst Controllers
6. The requirements manner and form in which application is to be made for license to issue DSC.
7. The period of validity of the license
8. The qualification and experience of an adjudicating officer as well as other officers
9. The salary, allowances and terms & conditions of service of the Presiding Officer etc.

Procedure

- Every notification shall be laid before each house of the parliament for a total period of 30 days.
- If both the houses, after the period of 30 days, agree the notification, it shall come into effect.

Power of State Government to make rules

The State Government is empowered to make rules regarding the following matters:

1. The electronic form in which filing, issue, grant, receipt or payment shall be effected in respect of use of electronic records and digital signature in government and it's agencies,
2. The manner in which such electronic records shall be filled or issued and fee or charges in connection with the same
3. Any other matter required to be provided by rules of the State Government

Section 89: ***Power of Controller to make regulations.***

The controller is empowered to make regulations under the Act with the previous approval of Central Government and in consultation with Cyber Regulations Advisory Committee on the following matters:

1. The particulars relating to maintenance of database containing the disclosure record of every Certifying Authority,
2. The conditions and restrictions subject to which the Controller may recognize any Foreign Certifying Authority
3. The terms and conditions subject to which a license may be granted
4. Other standards to be observed by a certifying authority
5. The manner in which the Certifying Authority may make the disclosure u/s 34
6. The particulars of statement to be submitted along with an application for the issue of a DSC.
7. The manner in which the subscriber should communicate the compromise of private key to the Certifying Authority.

**

CHAPTER 17

AUDIT OF (ACCOUNTING) INFORMATION SYSTEMS

AUDITING CONCERNS

- ➔ Auditors involved in reviewing an information system should focus their concerns on the system's control aspects. They must look at the total systems environment.
- ➔ Auditors should ensure that **Provisions** are made for:
  - **a.** An adequate trail to trace transactions,
  - **b.** Controls over the accounting for all transactions and controls to ensure their integrity throughout the computerized segment.
  - **c.** Handling exceptions to and rejections from the computer system.
  - **d.** Testing to determine whether the system perform as stated
  - **e.** Control over changes to the computer system
  - **f.** Authorization procedures for system overrides
  - **g.** Adherence to organizational and governmental policies on system implementation
  - **h.** Training user personnel in the operation
  - **i.** Developing detailed evaluation criteria to check whether implemented system meets the specifications
  - **j.** Adequate controls between interconnected computer systems
  - k. Adequate security procedures to protect user data
  - l. Backup and recovery procedures
  - m. Technology provided by different vendors
  - n. Databases are adequately designed and controlled.
- ➔ Thus the auditor is primarily concerned with adequate controls to safeguard the organization's assets.
- ➔ **The Computer Auditing Approach** ***(Reasons for Ineffectiveness of Audit Methods Used in the Audit of a Manual System)***
  - *a. Electronic Evidence:* essential evidence is not physically retrievable
  - *b. Terminology:* terminology used may be difficult for the Non EDP auditor to understand
  - *c. Automated Processes:* it may be difficult for the non EDP auditor to comprehend processing concepts and the logics of these concepts.
  - *d. New Risks and Controls:* threats to computer system and countermeasures are new to the non EDP auditor.

e. *Reliance on controls:* in a manual system the auditor can place some reliance on hard copy evidence regardless of the adequacy of controls. However in automated systems, electronic evidence is only as valid as the adequacy of controls.

➔ **The IS Audit's Scope and Objectives**

The auditor should first clearly identify the scope and objectives of the audit and for this he may focus on one or more of the following ***review areas***:

1. *Computerized Systems and Applications*
   The auditor should verify that the systems and applications are appropriate to the users' needs, efficient and adequately controlled to ensure valid, reliable, timely and secure input processing and output at current and projected levels of system activity.
2. *Information Processing Facilities:*
   Such facilities should be controlled to ensure timely, accurate and efficient processing
3. *Systems Development:*
   a. The auditor should ensure that system under development meet the system specifications,
   b. System under development is adequately tested and installed in accordance with generally accepted standards.
4. *Management of Information Systems:*
   Auditor should check the organizational structure and procedures to ensure a controlled and efficient environment for information processing.
5. *C/S, Telecommunications and Intranets:*
   Auditors must check the controls established on:
   - Client,
   - Server, and
   - Network.

   Auditors should provide the same level of control assurance in an Internet/Intranet environment as in a C/S environment. The emphasis should be on 2 key protocols: TCP/IP and HTTP.

➔ **The IS Auditor's Role**

- The purpose of IS Audit is to review and evaluate the internal controls that protect the system.
- He is responsible for establishing control objectives that reduce or eliminate potential exposure to control risk
- He must review the audit subject and evaluate the results of the review to determine areas that require correction and improvement.
- He should recommend actions that will provide a reasonable level of control over the assets of the company.

- ***Objectives of IS Audit***
  1. Computer security: security provisions protect computer resources
  2. Program development and acquisition
  3. Program modifications: authorization and approval my management.
  4. Processing of files, transactions etc are accurate and complete.
  5. Inaccurate or improperly authorized source data is identified and handled accordingly.
  6. Computer data files are accurate, complete and confidential.

A. COMPUTER SECURITY *(FRAMEWORK FOR AUDIT)*

1. Types of security errors and fraud faced by companies
- Theft or accidental damage to hardware, software or files
- Loss or unauthorized disclosure of sensitive data
- Unauthorized modification of programs and files
- Interruption of crucial business activities

2. Control Procedures to minimize security errors and fraud
- Developing information security/protection plan
- Restricting physical and logical access to hardware, software and data files.
- Encrypting data files
- Use of antivirus software, firewalls, backup procedures etc
- Developing a disaster recovery plan
- Information system insurance

3. Audit Procedures: System review
- Inspecting computer sites
- Interviewing personnel
- Reviewing logical access policies and procedures
- Review written documentation about physical access policies
- Examine system access logs, disaster recovery plan, casualty insurance policies, data storage and transmission policies.
- Review system backup procedures

4. Audit Procedures: Tests of controls
- Observe computer site access procedures and preparation of off-site storage of backup files.
- Review records of password assignment and modification
- Investigate how unauthorized access attempts were dealt with
- Verify the extent of data encryption in use, the use of data transmission controls, firewalls, anti-virus packages etc.
- Verify the use of preventive maintenance and amounts.

5. Compensating Controls
    - Sound personnel policies: segregation of duty etc
    - Effective user controls
    - Segregation of incompatible duties

B. PROGRAM DEVELOPMENT AND ACQUISITION

1. Types of Errors and fraud
    - Inadvertent programmed errors due to misunderstanding system specifications or careless programming, and
    - Unauthorized instructions deliberately inserted into the programs
2. Control Procedures to minimize errors
    - Management authorization for program development and approval of programming specifications
    - User approval of programming specifications
    - Testing
    - User acceptance testing
    - Documentation
3. Audit Procedure: System review
    - Independent and concurrent review of the system development process
    - Review system development policies and procedures, system authorization and approval policies, programming evaluation standards, program documentation standards, program testing and test approval procedures, final application system documentation etc
    - Discuss system development procedures with management, users and IS personnel.
4. Audit Procedure: Tests of control
    - Interview users about their involvement in system design and implementation
    - Review minutes of development, team meetings for evidence of involvement
    - Verify management and user sign-off at misc points in the development process
    - Review test specifications, test data and results of system tests
5. Compensating Controls
    - Strong processing controls
    - Independent processing of test data by auditor

C. PROGRAM MODIFICATION

1. Types of Errors and fraud
   - Inadvertent programmed errors due to misunderstanding system specifications or careless programming, and
   - Unauthorized instructions deliberately inserted into the programs
2. Control Procedures to minimize errors
   - Listing of program components that is to be modified
   - Management authorization and approval of program modifications
   - User approval of program change specifications
   - Testing of program changes
   - Complete program change documentation
   - Separate development, test and production versions of program
   - Logical access controls
   - Changes implemented by personnel independent of users and programmers
3. Audit Procedure: System review
   - Review program modification policies, standards and procedures
   - Review documentation standards for program modification
   - Review program modification testing and test approval procedures
   - Review final documentation for some typical program modification, test specifications, test data etc
   - Review logical access control procedures
4. Audit Procedure: Tests of control
   - Verify user and IS management approval for program changes
   - Verify that
     - Program components to be modified are identified and listed
     - Program changes test procedures comply with standards
     - Program change documentation complies with standards
     - Logical access controls are in effect for programmed changes
   - Observe program change implementation
   - Test for unauthorized or erroneous program changes using
     - *Reprocessing:* On a surprise basis the auditor uses the program (original source code) to process data and compares that output with the company output.
     - *Parallel simulation:* The auditor writes a program and compares the outputs from that with company output.
     - *Source code comparison:* The auditor keeps the original source code and frequently checks the current program source code with it using a source code comparison software.

5. Compensating Controls
    - Independent audit tests for unauthorized program changes
    - Strong processing controls

D. COMPUTER PROCESSING

1. Types of Errors and fraud
    - Failure to
        - Detect incorrect, incomplete or unauthorized input data
        - Correct errors flagged by data editing procedures
    - Introduction of errors into files during updating
    - Improper distribution or disclosure of output
    - Intentional or unintentional report inaccuracies
2. Control Procedures to minimize errors
    - Verification of computer data editing routines
    - Proper use of internal and external file labels
    - Reconciliation of batch totals
    - Effective error correction procedures
    - Supervision of computer operations
    - Effective handling of data input and output by data control personnel
    - Maintenance of proper environmental conditions in computer facility
3. Audit Procedure: System review
    - Review of
        - Administrative documentation for processing control standards
        - Systems documentation for data editing and other processing controls
        - Operating documentation for completeness and clarity
        - Copies of error listings, batch total reports and file change lists
    - Observe computer operations and data control functions
    - Discuss processing and output controls with operators and IS supervisory personnel
4. Audit Procedure: Tests of control
    - Evaluate adequacy of
        - Processing control standards and procedures
        - Data editing procedures
    - Verify processing accuracy for
        - A sample of sensitive transactions
        - Selected computer generated transactions
    - Reconcile a sample of batch totals and follow up on discrepancies
    - Search for erroneous or unauthorized code via of analysis of program logic.

- Verify
  - Adherence to processing control procedures
  - That selected application system output is properly distributed
  - Reported errors are handled accordingly
- Check for accuracy and completeness of processing controls using test data
- Monitor on-line processing systems using concurrent audit techniques
- Recreate selected reports to test for accuracy and completeness

5. Compensating Controls
   - Strong user controls
   - Effective source data controls

➔ The purpose of these audit procedures is to gain an understanding of the controls, evaluate their adequacy and observe operations for evidence that the controls are actually being followed.

➔ **Techniques Used to Test Processing Controls**

- ***Test Data Processing***
  - Here a hypothetical series of valid and invalid transactions are used to check that the program processes valid transactions accurately and does not process invalid transactions.
  - All logic paths should be checked for proper functioning by one or more of the test transactions
  - Test data can be generated from/by a listing of actual transactions, test data used by the programmer and a test data generator program.
  - *Batch Processing System:* here the company's program and a copy of relevant files are used to process test data.
  - *On-Line System:* the auditor enters the test data using a data entry terminal and observes and logs the system's responses.
  - *Disadvantages*
    - Preparation of test data is time consuming and requires a lot of effort
    - The test data may affect the company's actual files if necessary precautions are not taken.
- ***Concurrent Audit Techniques*** *(Used in On-Line Systems)*
  - Since on-line systems process transactions continuously, it's difficult to stop the system to perform audit tests.
  - Auditor uses Concurrent Audit techniques to:
    - Continuously monitor the system, and
    - Collect audit evidence while live data are processed.

- They use *Embedded Audit Modules* (program segments that perform audit functions).
- Such techniques are time consuming and difficult to use.
- ***Commonly Used Concurrent Audit Techniques***

1. An Integrated Test Facility (ITF)

- It places a small set of fictitious records in the master file. Such records may represent a fictitious department or division.
- Fictitious and actual records are processed together.
- The system must
  - Distinguish ITF records from actual records,
  - Collect information on the effects of such test transactions,
  - Report the results.
- *Advantages*
  - Eliminates the need to reverse the test transactions
  - Easily concealed from employees
  - Suited in on-line system as test transactions can be submitted on a frequent basis with actual transactions and traced throughout every processing stage.

2. Snapshot Technique

- Selected transactions are marked with a special code that triggers the snapshot process. It examines the way transactions are processed.
- Snapshot records the transactions and their master file records before and after processing and data is recorded in a Snapshot file and submitted to auditor for review.

3. SCARF (System Control Audit Review File) / Audit Log

- It uses embedded audit modules to continuously monitor transaction activity and collect data on transactions with special significance. Such data are recorded in SCARF file.
- The auditor receives a printout of SCARF file for review.

4. Audit Hooks

- Audit Hooks are audit routines that flag suspicious transactions.
- Using audit hooks, auditors can be informed of questionable transactions as soon as they occur.

5. Continuous and Intermittent Simulations (CIS)

- It embeds an audit module in DBMS. It examines all transactions that update the database.

- If a transaction has special audit significance, the module independently process data, records the results and compares it with those obtained from DBMS.
- Discrepancies are noted in a log file for subsequent review.

➢ ***Analysis of Program Logic*** *(Used as last resort)*

- Analysis of program logic is carried out when the auditor suspects that the application program contains unauthorized code or serious errors
- ***Software Packages Used***

1. *Automated Flowcharting Programs:* Interpret source code and generate a corresponding program flow chart.
2. *Automated Decision Table Programs:* generate a decision table representing the program logic.
3. *Scanning Routines:* searches a program for occurrences of a specified variable name or other character combinations.
4. *Mapping Programs:* identify unexecuted program code.
5. *Program Tracing:* prints all application program steps executed during a program run. This can be used to observe precise sequence of events that unfold during program execution. Auditors can detect incorrect logic paths, unexecuted code and unauthorized program

E. SOURCE DATA CONTROLS

1. Types of Errors and fraud

- Inaccurate source data
- Unauthorized source data

2. Control Procedures

- Effective handling of source data input by data control personnel
- User authorization of source data input
- Reconciliation of batch control totals
- 'Check digit' verification
- Use of turnaround documents.
- Computer data editing routines
- Logging off the receipt, movement and disposition of source data input.
- Effective procedures for correcting and resubmitting erroneous data.

3. Audit Procedure: System review

- Review
  - Documentation about responsibilities of data control function
  - Administrative documentation for source data control
  - Methods of authorization and examine authorization signatures

- Accounting systems documentation to identify source data content, processing steps and source data controls used.
- Document accounting source data controls using input control matrix
- Discuss source data control procedures with data control personnel, IS Management and users.

4. Audit Procedure: Tests of control
   - Observe and evaluate data control department operations and specific data control procedures
   - Verify proper maintenance of use of data control log
   - Evaluate how items are recorded in error log are dealt with
   - Examine samples of accounting source data for proper authorization
   - Reconcile a sample of batch totals
   - Trace how errors are dealt with.
5. Compensating Controls
   - Strong user controls
   - Strong processing controls.

➔ In an on-line system, the source data entry and processing functions are one operation. Hence source data controls are integrated with processing controls.

➔ *Input Control Matrixes* are used to show the control procedures applied to each field on input record and are used to review source data controls.

➔ Auditor should make sure that
   - The data control function is independent of other functions,
   - Data control log is maintained
   - Errors are properly handled, and
   - Overall efficiency of operations is ensured.

F. DATA FILES

1. Types of Errors and fraud
   - Destruction of stored data (hardware/software malfunction or sabotage)
   - Unauthorized modification or disclosure of stored data
2. Control Procedures
   - Secure file library and restrictions on access to data files
   - Logical access restrictions to data files
   - Proper use of file labels and write protection mechanisms
   - Concurrent update controls
   - Data encryption
   - Virus protection software

- Maintenance of backup copies
- Use of checkpoint and rollback policies to facilitate system recovery

3. Audit Procedure: System review

- Review
  - Documentation for functions of file library operation
  - Logical access policies and procedures
- Review operating documentation to determine prescribed standards for
  - Use of file labels and write-protection mechanisms
  - Use of anti-virus software
  - System recovery (checkpoint and rollback)
- Review systems documentation to examine prescribed procedure for
  - Use of concurrent update controls and data encryption
  - Control of file conversions
  - Reconciling master file totals with independent control totals
- Examine disaster recovery plan
- Discuss data file control procedures with IS management and operators

4. Audit Procedure: Tests of control

- Observe and evaluate file library operations
- Review records of password assignment and modification
- Observe and evaluate file handling procedures by operating personnel
- Observe computer site access procedures and preparation of off-site storage of backup files.
- Observe the procedures used to control file conversion
- Reconcile master file totals with separately maintained control totals
- Verify
  - the use of anti-virus software
  - the use of concurrent update controls and data encryption
  - completeness, currency and testing of disaster recovery plan

5. Compensating Controls

- Strong user controls
- Effective computer security controls
- Strong processing controls.

**

CHAPTER 18

INFORMATION SECURITY

INFORMATION SECURITY

- Security refers to the protection of valuable assets against loss, disclosure or damage, sabotage or natural disaster etc. with physical safeguards such as locks and logical or technological safeguards such as passwords.
- The valuable assets of the company includes the data or information recorded, processed, stored, shared, transmitted or retrieved from an electronic medium.
- Data protection is achieved through a layered series of technological and non technological safeguards.

> **Security Objective:** The protection of the interests of those relying on information, and the information systems & communications that delivers the information from harm resulting from failures of availability, confidentiality and integrity.

- The security objective is met when:
  - Information system is available and used when required (***Availability)***
  - Data and information is disclosed only to those who have a right to know ***(Confidentiality)***
  - Data and information are protected against unauthorized modification ***(Integrity)***
- Thus any information security procedure should satisfy availability, confidentiality and integrity.
- **Sensitive Information**
  - *Strategic plans* as these give an insight into competitors intentions
  - *Business Operations* consists of an organization's process and procedures most of which are deemed to be proprietary. This information may provide a market advantage to the organization.
  - *Finances* consists of accounts, cost details, employee compensation policies etc.
- **Establishing Better Information Protection: Steps to Keep Information Protected**
  1. Determining the value of different types of information.
  2. Identifying valuable information assets.
  3. Develop an access control methodology (which extend to file level)
  4. Protection of information stored on magnetic media such as hard drives, floppies etc
  5. Review of hard copy output of employees' daily work. (protecting paper documents)

- **Information Protection: Refocus**
  - Information protection includes electronic information held on, processed by or created on computers and paper documentation
  - Paper based information sources should be scanned to an electronic format immediately on receipt, creation or annotation so that currently existing mechanisms for protecting electronically held information can protect this information.
  - Paper based information is often not considered as valuable information.

PRINCIPLES OF INFORMATION SECURITY

1. **Accountability**
   - Responsibility and accountability must be explicit.
   - Accountability and responsibility should be fixed among data owners, process owners, technology providers and users.
   - *Issues to Consider*
     i. Specification of ownership of data and information
     ii. Identification of users and others who access the system
     iii. Recording of activities through the provision of management audit trails
     iv. Assignment of responsibility for maintenance of data and information
     v. Institution of investigative and remedial procedures when a breach is attempted.

2. **Awareness**
   - Awareness of risks and security initiatives must be disseminated
   - Data owners, process owners, users, technology providers and other parties with a legitimate interest to learn or be informed must be able to gain knowledge of
     i. The existence and general extent of the risks facing the organization and its systems, and
     ii. The organization's security initiatives and requirements.
   - *Issues to Consider*
     i. Level of detail disclosed must not compromise security
     ii. Appropriate knowledge is available to all legitimate parties
     iii. Creating awareness as part of induction program of new recruits
     iv. Recognition that maintaining awareness is an on-going process.

3. Multidisciplinary

- Security must be addressed taking into consideration both technological and non-technological issues.
- Technical standards should be developed with, and be reinforced by, codes of practice, audit, legislative, legal and regulatory requirements and awareness, education & training.
- *Issues to consider*
    i. Business value or sensitivity of information asset
    ii. Impact of the organizational and technological changes on the administration of security
    iii. Technologies available to meet the security objectives
    iv. Requirement of legislation and industry norms, and
    v. Requirements to carefully manage advanced security techniques.

4. Cost effectiveness

- Security must be cost effective. Security levels and associated costs must be compatible with value of the information.
- *Issues to consider*
    i. Value to and dependence of the organization on a particular information asset,
    ii. Value of the data or information based on pre-defined level of confidentiality or sensitivity
    iii. Threats to the information and the probability of occurrence
    iv. Safeguards to minimize or eliminate such threats with cost details
    v. Costs and benefits of incremental increases to the level of security
    vi. Safeguards that provide optimum balance between protection and related costs
    vii. If appropriate, the benefit of adopting established minimum security safeguards as cost effective alternative.

5. Integration

- Security must be coordinated and integrated (a coherent system).
- Measures, practices and procedures for the security of information should be coordinated and integrated with
    - Each other, and
    - Other security measures of the organization and third parties on whom the organization's business process dependent.

- *Issues to consider*
  i. Security policy and management should be included as an integral part of overall management.
  ii. Harmonization of all security procedures and processes (with information system)
  iii. Review of inter-related systems to ensure that the level of security is compatible, and
  iv. Risks relating to third parties on whom the organization's business processes depend.

6. Reassessment

- Security must be reassessed periodically as information system and the requirements for their security vary overtime.
- *Issues to consider*
  i. Increase in dependence on IS requiring an upgrade to the business continuity plans and arrangements.
  ii. Changes to the information systems and their infrastructure
  iii. New threats to the information system requiring better safeguards
  iv. Emerging security technologies providing more cost effective safeguards than were possible earlier, and
  v. Different business focus or organizational structure or legislation necessitating a change in the existing level of security.

7. Timeliness

- Security procedures must provide for monitoring and timely response.
- Procedures must be established to monitor and respond to real or attempted breaches in security in a timely manner in proportion to the risk.
- Swift reaction may be necessary in many cases.
- *Issues to consider*
  i. Instantaneous and irrevocable nature of business transactions
  ii. Volume of information generated from increasingly interconnected and complex information system
  iii. Automated tools to support real time and after the fact monitoring, and
  iv. Expediency of escalating breaches to the appropriate decision making level.

8. **Societal Factors**
    - Ethics must be promoted by respecting the rights and interests of others.
    - *Issues to consider*
        i. Ethical use and/or disclosure of data or information obtained from others
        ii. Fair presentation of the data or information to users, and
        iii. Secure destruction of data or information that is sensitive but no longer required.

PROTECTING COMPUTER HELD INFORMATION

- **Basic Rules For Protection of Computer-held Information**

First Rule: To know what is the information and where it is located.

Second Rule: To know the value of information held and how difficult it will be to recreate if it were damaged or lost.

Third Rule: To know who is authorized to access the information and what they are permitted to do with the information.

Fourth Rule: To know how quickly information needs to be made available should it become unavailable for any reason.

- **Types of Protection That an Organization Can Deploy**

1. ***Penetrative Information Protection***
    - This type of protection uses physical, logical and administrative security controls.
        i. *Physical Controls :* doors, locks, safes etc
        ii. *Logical Controls:* passwords, access controls
        iii. *Administrative Controls:* security awareness, user account revocation policy etc.
2. ***Restorative Information Protection***
    - Restorative information protection plans aim at restoring the information lost or damaged as a result of security violation. It's the second line of defense.
    - Creating backup is not enough. Organization should implement procedures to ensure accuracy of backup files and effectively recover lost files and information from backup files.
3. ***Holistic Protection***
    - Protection must be done holistically and give the organization the appropriate level of security at an acceptable cost.
    - An organization need to deploy both penetrative and restorative information protection procedures.

BEST APPROACH TO IMPLMENT INFORMATION SECURITY (STEPS INVOLVED)

- **Security Policies**
  - Every organization should have a security policy that defines acceptable behaviors and the reaction of the organization when such behaviors are violated.
  - It defines ways in which resources in a computer system may be accessed and used.
  - Commercial, competitive and legislative pressures require the implementation of proper security policies.
  - A good security policy should suggest procedures and policies that can prevent losses and also help in saving money and increasing productivity.
  - It should support and complement existing organizational policies.
  - The thrust of the policy statement must be to recognize the underlying value of, and dependence on, the information within the organization.
- **Policy Development**
  - The security objective and core principles provide a framework for the first critical step of security policy development.
  - ***Contents of Security Policy (Not Exhaustive)***
    i. Importance of information security to the organization

ii. Statement from the CEO in support of the goals and principles of effective information security
iii. Asset classification
iv. Data security
v. Personnel security
vi. Communication security
vii. Legal requirements
viii. Business continuity plans
ix. Definitions of responsibilities and accountability for information security
x. Reporting responsibilities
xi. Security awareness, training and education.

- **Roles and Responsibilities**
  - For security to be effective, individual roles, responsibilities and authority must be clearly defined, communicated and understood by all.
  - Responsibilities to consider include:
    - *Executive management* – overall responsibility for the security of information
    - *Information systems security professionals* – responsible for design, implementation, management and review of the organization's security policy, standards, measures, practices and procedures.
    - *Data owners* – responsible for determining sensitivity or classification levels of the data and maintaining accuracy and integrity of the data resident on the information system.
    - *Process owners* – responsible for ensuring that appropriate security, consistent with the organization's security policy, is embedded in their information system.
    - *Technology providers* – responsible for assisting with the implementation of information security.
    - *Users* – responsible for following the procedures set out in the organization's security policy, and
    - *Information systems auditors* – responsible for providing independent assurance to management on the appropriateness of the security objectives and on whether the security policy, standards, measures, practices and procedures are appropriate and comply with the organization's security objectives.

- **Design**
  - It refers to development of security and control framework consisting of standards, measures, practices and procedures within each system.
  - Individual business requirements and risks related to the particular system should be considered in order to identify the specific security requirements.

- Assessment of the risks must include both
  - Business and technical risks and
  - The analysis of control objectives, standards and techniques needed to provide an integral control framework.
- Design process concludes with the design of an integrated security system that is compatible with the needs of the organization.

➢ **Implementation**

- Once the solution is designed, it should be implemented on a timely basis and then maintained.
- ***Subject Areas Covered By Security Policy:*** **Standards, Measures And Procedures *(Various Information System Controls)***
  1. *Managerial controls* – span of control, separation of duties, training personnel etc.
  2. *Identification and authentication controls* – to establish accountability and to prevent unauthorized access.
  3. *Logical access controls* – to establish who or what has access to a specific type of information.
  4. *Accountability controls* – through management
  5. *Cryptology controls* – to ensure integrity of information transmitted or stored.
  6. *System development life cycle process controls* – to ensure that security is considered as an integral part of the process.
  7. *Physical and environmental controls* – to ensure that adequate measures are taken against threats emanating from the physical environment.
  8. *Computer support and operations controls* – to ensure that routine but critical activities like user support, software support, backups etc enhance the overall level of security.
  9. *Business community planning controls* – to ensure that an organization can prevent interruptions and recover and resume processing in the event of partial or total interruption to information system availability.

➢ **Monitoring**

- Monitoring measures are established to detect and ensure correction of security breaches. It's basic objective is to ensure that all actual and suspected breaches are promptly identified, investigated and acted upon. This will ensure ongoing compliance with policy, standards, and minimum acceptable security practices.
- ***Benefits***
  1. Enables prompt identification, containment of damage and expedient recovery.
  2. Increases the ability to prevent future damage and inconvenience.

3. Deterrence value of monitoring practices.
4. *Other Benefits*
    a. Refinement of security levels
    b. Initiation of
        - Reassessment programs
        - Intelligent monitoring system
        - Network or system penetration studies
    c. Changes to standards

- ***Effective Monitoring: Issues to be Addressed***
    - Appointment of a responsible manager
    - Independent and objective assessment of security controls
    - Establishment of clear and expedient investigative procedures
    - Assimilation and examination of audit trails from various system components
    - Timeliness of escalation processes
    - Dynamic business and information system environment.

➢ **Awareness, Training and Education**

- Personnel are often the most weakest link in securing information and hence they should be:
    - Made aware of the need to protect information,
    - Trained in the skills needed to operate securely, and
    - Educated in Security measures and practices.
- All the employees should be aware of the security policies and it's importance should be informed to all employees on a regular basis.
- ***Ways to Impart Awareness***
    - Training to all staffs
    - Non disclosure statements signed by the employees
    - Company newsletter
    - Periodic audits
    - Visible enforcement of security rules
    - Security drills
    - Pasting security policies on notice boards etc.
- ***Responsibilities of Employees with regard to Security***
    - Understanding the security policy
    - Maintaining secrecy of login ID and passwords
    - Duly reporting the security administrator of alleged violations of security
    - Ensuring that good physical security is maintained

- Non disclosure of access door locks combinations and questioning unfamiliar people.

- ***Benefits of Creating Awareness***
  i. Improves employee behavior and attitude towards information security, and
  ii. Increases the ability to hold employees accountable for their actions
- It should be noted that the level of training needed to be imparted depend upon the level of management the employee is in. i.e. when users are trained in basic security controls, System Administrators should be trained in advanced security controls.

SECURITY ADMINISTRATOR

- A Security Administrator is the person who is solely responsible for controlling and coordinating the activities pertaining to all security aspects of the organization.
- **Role of Security Administrator**
  - Security Administrator attempts to ensure the facilities in which systems are developed, implemented, maintained and operated are safe from threats
  - Security Administrator sets policy subject to management approval
  - He is responsible for establishing the minimum fixed requirement for classification of information based on the physical, procedural and logical security elements.
  - He investigates monitors and advice employees and management on matters pertaining to security.
  - Security Administrator guides other Security Administrators and users on the selection and application of security measures.
  - He trains other Security Administrators to mark and handle processes, select software packages and solves problems.
  - He investigates all security violations
  - Security Administrator advises senior management on matters of information resource control
  - He consults on matters of information security
  - He conducts a security program to evaluate facilities available
  - Security Administrator prepares possible threats to organization , prepare inventory of assets and evaluate existing controls.
- **Security Committee**
  - End users, executive management, security administration personnel, IS personnel and legal counsel members should be an integral part of the security committee.
  - The committee should discuss the policies and procedures regarding security periodically.

SOME KEY DEFINITIONS

- **Information System Auditor:** He is an internal or external auditor who possesses the knowledge, skill and abilities to review and evaluate the development, maintenance and operation of components of information system.
- **Integrity:** The characteristic of data and information being accurate and complete and the preservation of accuracy and completeness by protecting the data and information from unauthorized, unanticipated or unintentional modification.
- **Cyberspace:** the global information and communications network where time, distance and space are not a limitation.

**

CHAPTER 19

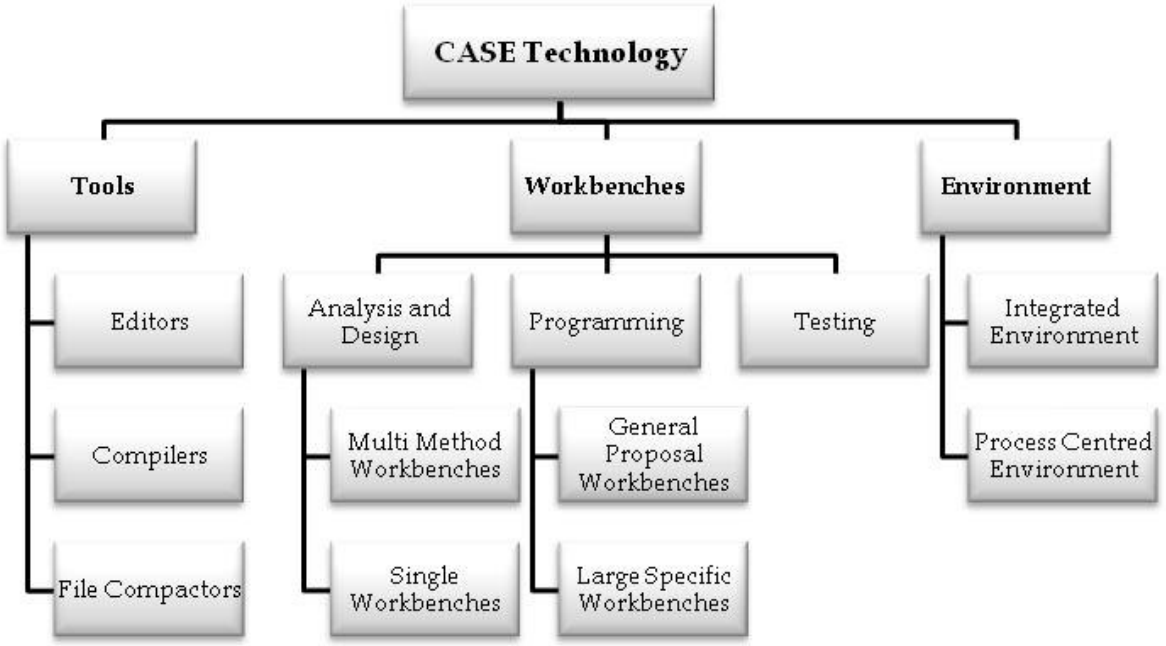
USE OF SIMPLE CASE TOOLS, ANALYSIS OF FINANCIAL STATEMENTS USING DIGITAL TECHNOLOGY

CASE TOOLS

- CASE stands for 'Computer Aided Software Engineering'. CASE provides the software engineer with the ability to automate manual activities and to improve engineering insight.
- CASE tools ensure that quality is designed in before the product is built.
- Simply put CASE tools are automated software tools. It encompasses computer-based procedures, techniques and tools which can be used to develop, maintain and reengineer software.
- CASE tools can be used as a single tool, or they can be integrated into a common framework of environment such as Integrated Project Support Environment (IPSE) where a team of software engineers work together to produce software.
- All dimensions of software engineering comes together to form integrated environments.
- ***Components of Integrated Environments***
    1. *Analysis Dimension*: planning systems, defining requirements and designing systems.
    2. *Development Dimension*: traditional programming development tools.
    3. *Management Dimension*: this provides methods and tools needed to manage and ctrl projects.
    4. *Support Dimension*: tools and techniques needed to sustain existing software programs.

CASE CLASSIFICATION

- CASE technology allows different types of tools to be assessed and compared.
- There are 3 categories of CASE tools:
    1. Tools that support individual process tasks such as compiling a program, comparing test results etc
    2. Workbenches to support process phase such as specification, design etc.
    3. Environment support for all or part of software process.



Examples of different types of CASE tools

Tool Type	Example
Management tools	PERT Tools, estimation tools
Editing tools	Text editors, diagram editors
Configuration management tools	Version management system, change management system.
Prototyping tools	High level language tools, user interface generators
Method support tools	Design editors, data dictionaries, code generators
Language processing tools	Compilers, interpreters
Program analysis tools	Cross reference generators, static analyzers, dynamic analyzers
Testing tools	Test data generators, file compactors
Debugging tools	Interactive debugging system
Documentation tools	Page layout program, image editors
Reengineering tools	Cross reference system, program restructuring systems

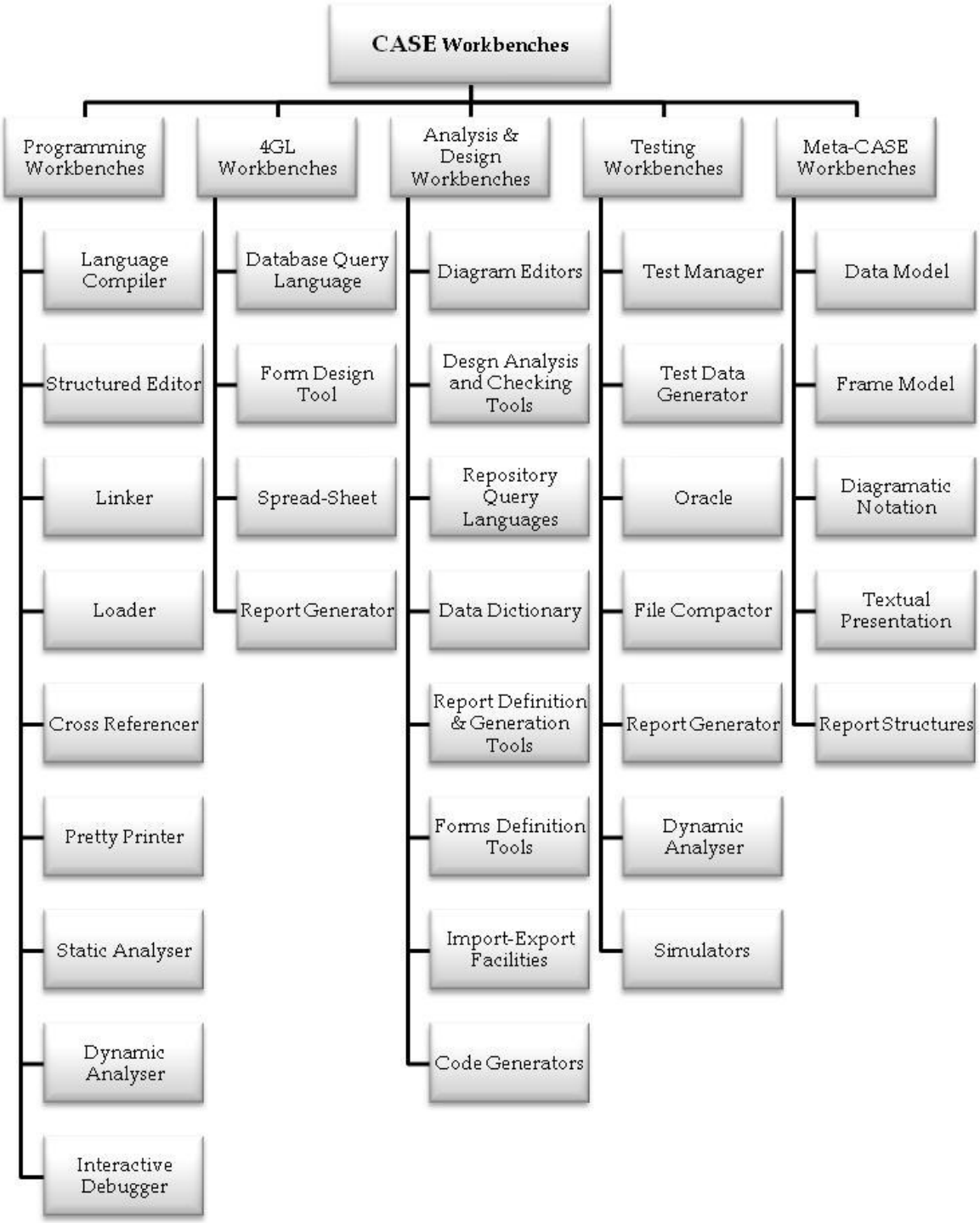
- **Integrated CASE Tools**

1. Specialized CASE tools can be combined together to provide a wider support to software process activities. There are ***five*** different levels of integration of CASE tools which are possible. These are:

   1. ***Platform integration***
      - The tools or workbenches to be implemented run on the same platform where platform means a single computer, OS or a network.
   2. ***Data Integration***
      - It's the process of exchange of data by CASE tools. The result from one tool can be passed on as input to another tool.
      - *Different Levels of Data Integration*
        i. Shared Files: all tools recognize a single file format.
        ii. Shared Data Structure: tools make use of a shared data structure which usually include program or design language information.
        iii. Shared Repository: tools are integrated around an object management system which includes a public share data model describing the data entities and relationships which can be manipulated by tools.
   3. ***Presentation/User Interface Integration***
      - The tools in the system use a common metaphor or style and a set of common standards for user interaction.
      - *Different Levels of Presentation Integration*
        i. Window system integration: tools integrated at this level use the same underlying window system and present a common interface for window manipulation commands.
        ii. Command Integration: tools use the same form of commands for comparable functions.
        iii. Interaction Integration: its related with the direct manipulation interface where the user interface interacts with a graphical or textual view of the entity.
   4. ***Control Integration***
      - Control integration is the mechanism of one tool in a workbench or environment to control the activation of other tools in the CASE system. The tool is able to start and stop other tools.
   5. ***Process Integration***
      - The CASE system has embedded knowledge about the process activities, their phasing, their constraints and the tools needed to support their activities.

- Process integration requires that the CASE system maintains a method of the software process and uses this mould to drive the process activities.
- Activities and deliverables are identified, a coordination strategy defined and the tools required to support activities are specified.

CASE WORKBENCHES



- CASE workbenches are available to support most software process activities.
- **Types of CASE Workbenches**
  1. ***Software Development Workbench:*** Used for analysis and design, programming and program testing.
  2. ***Cross Development Workbench:*** This type of workbench supports host target working where software is developed on one machine for execution on another system.
  3. ***Configuration Management Workbench:*** Supports configuration management.
  4. ***Documentation Workbench:*** Supports production of high quality documents.
  5. ***Project Management Workbench:*** Supports project management activities.
  6. ***Programming Workbenches***: It consists of tools that support the process of program development. Some of such tools are:
     - *Language Compiler:* translates host program to object code.
     - *Structured Editor:* incorporates embedded programming language knowledge and edits the syntax representation of the program in the AST rather than its source text.
     - *Linker:* links the object code program with components which have already been compiled.
     - *Loader:* loads the executable program into the computer memory prior to execution.
     - *Cross Referencer:* produces a cross reference listing showing where all program names are declared and used.
     - *Pretty Printer:* scans the AST and prints the source program according to embedded formatting rules.
     - *Static Analyzer:* analyses the source code to discover uninitialized variables, unreachable code, uncalled functions and procedures etc.
     - *Dynamic Analyzer:* produces a software code listing annotated with number of times each statement was executed when the program was run. It also generates information on program branches and loops and statistics of processor usage.
     - *Interactive Debugger:* allows the user to control the execution sequence and view the program state as execution progresses.
  7. ***4GL Workbenches:*** these are geared towards producing interactive application which relies on extracting information from an organizational database. The tools included in this are:
     - *Database Query Language:* E.g. SQL
     - *Form Design Tool:* used to create forms for data input and display
     - *Spread-Sheet:* used for the analysis and manipulation of numeric information.
     - *Report Generator:* used to define and create reports from information in database.

8. ***Analysis & Design Workbenches***
    - *Diagram Editors:* used to create dataflow diagrams, structured charts etc
    - *Design Analysis and Checking Tools:* used to process the design and then submit report on errors and anomalies. These tools are generally integrated with editing system.
    - *Repository Query Languages:* allows the designer to find designs and associate design information in the repository.
    - *Data Dictionary:* maintains information about the entities used in a system design.
    - *Report Definition & Generation Tools:* it takes information from the central store and automatically generates system documentation.
    - *Forms Definition Tools:* allows screen and document formats to be specified.
    - *Import-Export Facilities:* it allows the interchange of information from the central repository with other development tools.
    - *Code Generators:* it generates code or code skeletons automatically from the design captured in the central store.
9. ***Testing Workbenches:*** These are open systems which evolve to suit the needs of the system being tested. It includes:
    - *Test Manager:* manages the running and reporting of program tests. It keeps track of data.
    - *Test Data Generator:* generates test data for the program being tested by using patterns to generate random data of the correct form.
    - *Oracle:* generates predictions of expected results.
    - *File Compactor:* compares the result of program tests with the previous test results and reports differences between them.
    - *Report Generator:* provides report definition and generation facilities for test results.
    - *Dynamic Analyzer:* adds code to a program to count the number of times each statement has been executed.
    - *Simulators:* includes target simulators, UI simulators, I/O simulators etc.
10. ***Meta-CASE Workbenches:*** These are used to generate other CASE tools. They are usually based on a description of the rules and notations of design or analysis method. Following are the five different aspects to be considered in Meta-CASE Workbench:
    - *Data Model:* for capture and output generation.
    - *Frame Model:* it defines the views of data model to be generated. Each possible view of the data model is termed as frame.
    - *Diagrammatic Notation:* for each diagram frame.
    - *Textual Presentation:* for each text frame.
    - *Report Structures.*

- **Typical Components of a CASE Workbench**
  1. *Diagram Editing System:* used to create dataflow diagrams, structured charts etc
  2. *Design Analysis and Checking Tools:* used to process the design and then submit report on errors and anomalies. These tools are generally integrated with editing system.
  3. *Query Languages:* that allow the user to browse the stored information and examine completed designs.
  4. *Data Dictionary:* maintains information about the entities used in a system design.
  5. *Report Definition & Generation Tools:* it takes information from the central store and automatically generates system documentation.
  6. *Forms Definition Tools:* allows screen and document formats to be specified.
  7. *Import-Export Facilities:* it allows the interchange of information from the central repository with other development tools.
  8. *Code Generators:* it generates code or code skeletons automatically from the design captured in the central store.
- **An Example of a CASE Tool Set: Various Tools**

CASE Tool Set	
Host Target Communication Software	Links the development computer to the computer on which the software is to execute (target machine)
Target Machine Simulation	Used in host machine to execute and test target machine software developed in a host machine.
Cross Compilers	These are language processing systems which execute on the host machine and generate code for the target machine.
Testing And Debugging Tools	It includes test drivers, dynamic and static program analyzers etc. debugging on the host of programs and executing on the target should be supported if possible.
Graphical Design Editors	These can be compared to those incorporated in CASE workbenches but are tailored to support a real time method.
Text Processors	It supports documentation development on the same machine as program development.
Project Management Tools	It allows estimates of the time required for a project and its cost. It also provide facilities for generating management reports on the status of a project at any time.

- The tool set also includes a number of tools for configuration management, change control, version control and variant management.
- It also provides text editing tools and e-mail system to support communications.
- ***CASE Environment:*** A CASE environment is a carefully configured and integrated system of automated tools applied to the entire software life cycle for each unique software development, maintenance or redevelopment problem.

**

CHAPTER 20

IMPORTANT QUESTIONS / AREAS

➔ **CHAPTER 1**

- Difference between open and closed system

➔ **CHAPTER 2**

- Transaction Processing Cycle.
- Common cycles of a business activity

➔ **CHAPTER 3**

- Potential impact of MIS on different levels of management
- MIS – prerequisites, features, limitation and constraints
- Main prerequisites of an effective MIS

➔ **CHAPTER 4**

- Definition of Personnel Information System, its various subsystems, benefits.
- Material Requirement Planning
- Financial information system

➔ **CHAPTER 5**

- EIS- meaning
- EIS Vs Traditional Information System
- DSS

➔ **CHAPTER 6**

- Client Server Model- features, components, benefits
- Risks in transition from mainframes to C/S Model

➔ **CHAPTER 7**

- Data Dictionary (Asked 5 times!!)
- Top down and Bottom up approaches and their differences
- Various system development approaches
- Prototyping- Advantages, disadvantages, steps involved in prototyping
- System development life cycle and activities involved

➔ **CHAPTER 8**

- Factors to be considered while designing user inputs and outputs
- Coding schemes- meaning and features of a good coding scheme
- Guidelines for efficient form design

➔ **CHAPTER 9**

- Stages of development of a program developed in house (program development life cycle)
- Application software: meaning
- Advantages of pre written software
- Factors on which 'make or buy' decision of application software depends.
- Benchmarking problem on vendors proposal

➔ **CHAPTER 10**

- System maintenance (asked 5 times!!)
- Conversion from manual to computerized system – strategies and activities involved
- Importance of personnel training

➔ **CHAPTER 11**

- Draw a diagram depicting the flow of information for computerized production scheduling system and explain the following:
  - System interfaces
  - Files and inputs
  - Output reports

➔ **CHAPTER 12**

- ERP: Meaning, Characteristics, Benefits, Evaluation criteria
- Implementation of CSF & KPI
- Business process re-engineering

➔ **CHAPTER 13**

- Transaction logs
- Firewalls
- General components of Disaster Recovery Plan
- Steps to be taken to ensure the software and data security in a computer department.
- Different types of security required for the computer system. Components of physical security of a computer installation.

➔ **CHAPTER 14**

- Validation controls

➔ **CHAPTER 15**

- Disc Imaging And Analysis Technique
- Internet fraud
- Computer fraud: Meaning and why it's a serious threat to a business.
- Computer fraud using input: what are the different ways?

➔ **CHAPTER 16**

- Digital Signature Certificates and Digital Signatures
- Objectives and scope of the Act
- Cyber Appellate Tribunal
- Please read carefully the following three scenarios and answer the questions given below:
    1. **Scenario 1:** Nobody told you that your internet use in the office was being monitored. Now you have been warned you will be fired if you use the net for recreational surfing again. What are your rights?
    2. **Scenario 2:** Your employees are abusing their internet privileges, but you don't have an internet usage policy. What do you do?
    3. **Scenario 3:** Employee Mr. X downloads adult material to his PC at work and employee Miss Y sees it. Miss Y then proceeds to sue the company for sexual harassment. As the employer are you liable?

Answer

- ***Scenario 1:*** When you are using office computer you have virtually no rights. You would have a tough time convincing the court that the boss invaded tour privacy by monitoring the use of company PC during office hours. You should probably be grateful that you got a warning stating that you will be fired if you use the internet for recreational surfing again.
- ***Scenario 2:*** Although the law Is not fully developed in this area courts are taking a straightforward approach. If it's a company computer the company can control the way in which it is to be used by its employees. You really don't need an internet usage policy to prevent inappropriate use of the computer. To protect the company in future, its advisable to distribute an internet usage policy to your employees as soon as possible to stop your employees from abusing their internet privileges.

- ***Scenario 3:*** Whether it comes from the internet or a magazine, adult material has simply no place in a office. So Miss Y could certainly sue the company for making her work in sexually hostile environment. The best defense for the company is to have as internet usage policy that prohibits employees to access adult sites. Of course, you have to follow up and monitor. Today, software is available for monitoring the employees whenever they visit adult sites. It will shut down the computer and alert the person who is monitoring the internet usage. If someone is caught browsing adult material in the office, you must at least send a written communication to the offending employee. If the company lacks a strict internet usage policy, Miss Y could prevail in the court.

➔ **CHAPTER 17**

- Integrated Test Facility
- IS Audit: Objectives and relevance
- A company is offering a wide range of products and services to its customers. It relies heavily on its existing information system to provide up to date information. The company wishes to enhance its existing system. You being the IS auditor, suggest how the investigation of the present information system should be conducted so that it can further be improved upon (May, 2006)

Answer: *(Refer Chapter 7, Page no 58 for details)*

- Investigation involves collecting, organizing and evaluating facts about the system and the environment in which it operates. Following areas should be studied in depth:
  - Review of historical aspects
  - Analyze input
  - Review data files
  - Review methods, procedures and communications
  - Analyze output
  - Review internal control
  - Model the existing system

- How does MIS auditing enhance control process (November, 2006)

Answer:

- MIS auditing helps organization to determine the effectiveness of the controls in their information system.
- MIS audits ensure a high level of completeness and accuracy of data stored.

- It identifies all existing controls and assesses its effectiveness.
- Auditor lists and ranks all control weaknesses and estimates the probability of their occurrences.
- He also assesses the financial and organizational impact of each threat.
- Then management can take appropriate steps to eliminate or reduce such threats.

➔ **CHAPTER 18**

- Information security: Meaning and principles of information security
- Contents of information security policy

➔ **CHAPTER 19**

- Short notes on CASE tools

➔ **RESIDUAL**

- Various methods by which internet can be accessed and the considerations for choosing an alternative.

Answer:

- *Methods to access Internet*
  1. ISP
  2. Online services
  3. Direct communication through a gateway
  4. Use of someone else's gateway
- *Points to be Considered*
  1. Whether accessing the internet for the company or limited official use at distant location
  2. Types of services needed
  3. Monthly usage time
  4. Budgeted spending
  5. Data rate wanted

- Security management steps an internet user should take to protect from Cyber crime and computer security threats

Answer

- Use anti virus and fire wall software and update it often
- Don't allow online merchants to store credit card information for further purchases
- Use a hard-to-guess password that contains alphabets, numbers and special characters.

- Use different passwords for different websites
- Confirm that the site through which you are doing business is a secure site.
- Use security programs that give you control over 'cookies' that send information back to website.
- Don't open e-mail attachments unless you know that the source of the incoming message is trustworthy.
- Use spam filters to filter unwanted or malicious e-mails.

**

! Best of Luck !