MANAGEMENT INFORMATION & CONTROL SYSTEMS

MICS NOTES Prepared by CA. Ashish Goyal, M.Com,
Reach me : ashishgoyalcaindore@gmail.com,

CA - FINAL GR II

CONTENTS

CHAPTER-1

BASIC CONCEPTS OF SYSTEMS

What is a System?

The term "System" may be defined as:

"A set of interrelated elements that operate collectively to accomplish some common purpose or goal".

Ex: Human body, a business and Computer based information system.

Human body:

Various parts such as head, heart, hands legs and so on.
These are related by means of connecting networks of blood vessels and nerves.
The goal is "living".

Business system:

Various components such as people, money, material, machines etc.
These are related and interacted by various organizational processes.
With a goal of converting organizational resources into products and services.

Computer based information system:

Various components such as people, hardware, software, data and procedures.
These are related and interacted by various ways.
With a goal of providing timely information to authorized people.

Thus 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.

TYPES OF SYSTEMS

Systems are classified based on the following factors:

1. According to components/elements.
2. According to behavior of the system.
3. According to level of interaction.

According to components/elements

Abstract and Physical

a. Abstract System: An abstract system is an orderly arrangement of interdependent ideas or constructs.
   Ex: A computer program.
b. Physical system is a set of elements which operate together to accomplish an objective.
   Ex: Production system, Transportation system etc.

According to behavior:

Deterministic and Probabilistic System

- A deterministic system operates in a predictable manner.
- The interaction among the parts is known with certainty.
- If one has a description of the state of the system at a given point of time plus a description of its operation, the next state of the system may be given exactly, without error.

An example is a correct computer program, which performs exactly according to a set of instructions.

- A probabilistic system can be described in terms of probable behavior.
- A certain degree of error is always attached to the prediction of what the system will do.

An inventory system is an example of a probabilistic system. The average demand, average time for replenishment, etc. may be defined, but the exact value at any given time is not known.

According to level of interaction

Closed and Open Systems

- Closed system
- Open system

Closed System:

- A "Closed system" is self-contained
- Does not interact or make exchange across its boundaries with its environment.
- A relatively closed system has least interaction with its environment.
- It rarely receives input from other systems.

Open System:

- An "Open system" actively interacts with other systems and establishes exchange relationships.
- Often they are forced to adapt themselves with the external environment for survival and growth.
- Organisations are considered to be relatively open systems.
- Organisations continuously interact with the external environment, by processes or transformation of inputs into useful output
- Organisations behave as relatively closed system in certain respects so as to preserve their identity and autonomy.

Organisations are open systems, because they are input output systems. The input consists of finance, physical and mental labor and raw material.

Organisations perform several operations on these inputs and process out products or services. Organisations are dependent upon their external environment for the inputs required by them and for disposing of their outputs in a mutually beneficial manner.

System Environment:

All systems function within some sort of environment. The environment like the system is a collection of elements. These elements surround the system and often interact with it. For any given problem, there are many types of systems and many types of environments.

- The features that define and describe a system form its **boundary.**
- The system is inside the boundary.
- The environment is outside the boundary.

A **subsystem** is a part of a larger system. Each system is composed of sub-systems, which in turn are made up of other subsystems, each sub-system being defined by its boundaries.

A **supra-system** refers to the entity formed by a system and other equivalent systems with which it interacts.

The interconnections and interactions between the subsystems are termed as **interfaces.** Interfaces occur at the boundary and take the form of inputs and outputs.

For example, an organisation may be subdivided into numerous functional areas such as marketing, finance, manufacturing, research and development, and so on. Each of these functional areas can be viewed as a subsystem of larger organisational system because each could be considered to be a system in and itself.

Further more, marketing may be viewed as a system that consists of elements such as market research, advertising, and sales and so on. Collectively, these elements in the marketing area may be viewed as making up the marketing supra-system. Similarly the various functional areas (subsystems) of an organisation are elements in the same supra-system within the organisation.

SUB SYSTEMS

The use of subsystems as building blocks is basic to analysis and development. This requires an understanding of the principles, which dictate how systems are built from subsystems. The basic principles to be considered before developing systems based on subsystem concepts:

1. Decomposition
2. Simplification
3. Preventing systems entropy
4. Systems stress and system change

1. Decomposition:

- A complex system is difficult to understand when considered as a whole.
- The system will be decomposed or factored into subsystems.
- The boundaries and interfaces are defined, so that the sum of the subsystems constitutes the entire system.
- This process of decomposition is continued with subsystems divided into smaller subsystems until the smallest subsystems are of manageable size.

The subsystems resulting from this process generally form hierarchical structures. In the hierarchy, a subsystem is one element of supra-system.

Decomposition into subsystems is used to analyze an existing system and to design and implement a new system. In both cases, the investigator or designer must decide how to factor, i.e., where to draw the boundaries. The decisions will depend on the objectives of the decomposition and also on individual differences among designers: the latter should be minimized.

An example of decomposition is the factoring of an information processing system into subsystems.
A business information system divided into subsystem such as:

a. Sales and order entry.
b. Inventory.
c. Production
d. Personnel and payroll
e. Purchasing
f. Accounting and control
g. Planning
h. Environmental intelligence

Each subsystem is divided further into subsystems. For example, the personnel and payroll subsystem might be divided into the following smaller subsystems.

a. Creating and update of personnel payroll records.
b. Payroll data entry and validation
c. Hourly payroll processing
d. Salaried payroll processing
e. Payroll reports for management
f. Payroll reports for government

If the task is to design and program a new system, the subsystems defined above might be further subdivided into smaller subsystems or modules.

2. Simplification: The process of decomposition could lead to a large number of subsystem interfaces to define. For example, four subsystems which all interest with each other will have six interconnections, a system with 20 subsystems all interacting will have 190 interconnections. The number can rise quite quickly as the number of subsystems increases. The number of inter connections if all subsystems interact is in general n(n-1)/2, where n= the number of subsystems. Each interconnection is a potential interface for communication among subsystems. Each interface implies a definition of a communication path.

Simplification is the process of organizing subsystems so as to reduce the number of interconnections. A method of simplification is given below:

1. Clusters of subsystems are established which interact with each other, then a single interface path is defined from the cluster to other subsystems or clusters of subsystems.

3. Preventing Systems Entropy:

- Systems can run down and decay or can become disordered or disorganized.
- In system terminology, an increase in entropy takes place.
- Preventing or correcting the increase in entropy requires inputs of matter and energy to repair, replenish, and to maintain the system.
- This maintenance input is termed negative entropy.

Open systems require more negative entropy than relatively closed systems for keeping at a steady state of organization and operation. Ex: In a computer program over a period of time the user might get dissatisfied with the features incorporated in the system, or the system itself producing errors, called systems entropy. The negative entropy or the maintenance of this system can be carried out by enhancing the features of the system, or correct the system.

4. System stress and system change

Systems, whether they may be living or artificial systems change because they undergo stress. A stress is a force transmitted by a system's supra-system that causes a system to change, so that the supra-system can better achieve its goals. In trying to accommodate the stress, the system may impose stress on its subsystems, and so on.

Types of Stress: There are two basic forms of stresses, which can be imposed on a system, separately or concurrently:

1. A change in the goal set of the system. New goals may be created or old goals may be eliminated.
2. A change in the achievement levels desired for existing goals. The level of desired achievement may be increased or decreased.

For example, the goal set for a computer system may change if a new requirement is imposed by management for system data be shared among multiple users rather than be available only to a single user.

Consequences of Stress: When a supra-system throw stress on a system, the system will change to accommodate the stress, or it will become pathological; that is, it will decay and terminate.

Process of Adaptation: Systems accommodate stress through a change in form; there can be structural changes or process changes. For example, a computer system under stress for more shareability of data may be changed by the installation of terminals in remote locations—a structural change. Demands for greater efficiency may be met by changing the way in which it sorts data—a process change.

INFROMATION:

It can be defined as '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. The quality of data determine quality of output i.e., information. This phenomenon is also known as garbage in garbage out (GIGO). The management plays the part of converting the information into actions through the familiar management process of decision making.

Characteristics of information: The important characteristics of useful and effective information are as follows:

1. *Timeliness:* It is a mere true to say that information, to be of any use, has to be timely. However, it is not always necessary that information is required at such a short interval. Usually, as we proceed from the lower levels to higher levels of management, the time interval necessary for providing decision influencing information on a routine or on exception basis increases.
2. *Purpose:* Information must have purposes at the time it is transmitted to a person or machine, otherwise it is simply data. Information communicated to people has a variety of purposes because of the variety of activities performed by them in business organizations. The basic purpose of information is to inform, evaluate, persuade, and organize.
3. *Mode and format:* The modes of communicating information in business are either visual, verbal or in written form.
   Format of information should be so designed that it assists in decision making, solving problems, initiate planning, controlling and searching. It should be simple and relevant, should highlight important points but should not be too cluttered up.
4. *Redundancy:* It means the excess of information carried per unit of data. However, in business situations redundancy may some time be necessary to safeguard against error in the communication process. For example, the correspondence in contracts may carry figure like '4' followed by (FOUR).
5. *Rate:* The rate of transmission/reception of information may be represented by the time required to understand a particular situation. For machines the rate may be based on the number of bits of information per character per unit of time or for humans may be the number of characters transmitted per minute.
6. *Frequency:* The frequency with which information is transmitted or received affects its value. Financial reports prepared weekly may show so little change that they have small value, whereas monthly reports may indicate changes big enough to show problems or trends.
7. Completeness: The information should be as complete as possible. With this complete information, the manager is in a much better position to decide whether or not to undertake the venture.
8. *Reliability:* The information presented to the top management should be a reliable one. The information which is arrived at should have an indication of the confidence level.
9. *Cost benefit analysis:* The benefits that are derived from the information must justify the cost incurred in procuring information.
10. *Validity:* It measures the closeness of the information to the purpose.
11. *Quality:* Quality refers to the correctness of information.

Value of Information: It is defined as difference between the value of the change in decision behavior caused by the information and the cost of the information. In other words, given a set of possible decisions, a decision-maker may select one on basis of the information at hand. If new information causes a different decision to be made, the value of the new information is the difference in value between the outcome of the old decision and that of the new decision, less the cost of obtaining the information.

BUSINESS INFORMATION SYSTEM:

The purpose of business information system, like any other system in an organisation, is to process input, maintain files of data about the organisation, and produce information (reports and other outputs). Information systems consist of sub-systems, including hardware, software and data storage for files and databases. The particular set of sub systems used - the specific equipment, programs, files and procedures constitutes an information system application.

CATEGORIES OF INFORMATION SYSTEMS:

Systems Analysts develop several different types of information systems to meet a variety of business information needs. The major categories are

- Transaction processing systems (TPS).
- Management Information systems (MIS).
- Decision support systems (DSS).
- Executive Information Systems (EIS).
- Expert systems (ES).

TRANSACTION PROCESSING SYSTEMS (TPS):

The most fundamental computer-based system in an organization is the business transaction processing system. The objective of a transaction processing system is to improve the effectiveness in day-to-day activities of a concern, which all organisations engage. Standard operating procedures, which facilitate handling of transactions, are often included in computer programs that control the entry of data, processing of details and search and presentation of data and information. The high volume of business transactions and specific procedures for handling them often requires the usage of computer systems. Transaction processing systems if computerized provide speed and accuracy and can be programmed to follow routines without any variance.

MANAGEMENT INFORMATION SYSTEMS

Transaction processing systems are operations oriented. In contrast, Management Information Systems (MIS) assist managers in decision-making and problem solving. They use results produced by the Transaction processing systems, but they also use other information. In any organisation, decisions must be made on many issues that recur regularly and require certain amount of information. The information systems can be developed so that the reports are prepared regularly to support these recurring decisions.

DECISION SUPPORT SYSTEMS:

Not all decisions are of recurring nature. Some occur only once or recur infrequently, Decision support systems are aimed at assisting managers who are faced with unique (non-recurring) decision problems. An important aspect of these decisions is determining what information is needed for decision making. As information is acquired, the manager may realize that additional information is required. In such cases, it is impossible to predesign system report formats and contents. A Decision Support System must have greater flexibility than other information systems.

The Decision Support System (DSS) is of much more use when the decisions are of an unstructured or semi-structured nature. In this situation the problem area is modeled and various alternatives explored. In its simplest form, the spreadsheet could be considered as decision support system. Models can be built using formulae, and variables can be changed to see what would be the results. Decision support systems should not been seen as stand-alone systems, they should be seen as integrated piece of software incorporating database, modelbase, and user interface (easy to use query language).

EXECUTIVE INFORMATION SYSTEMS (EIS):

These are designed primarily for the strategic level of management. They enable executives to extract summary data from the database and model complex problems without the need to learn or have high computing skills. The systems are easy to use, incorporating touch screens in some instances, and being graphical based. High-level summary data and trend analysis is provided at the touch of a button, using graphics as a way of presenting the information. There are standard models for these the executives do not need to construct the query or model. From the executive's PC, telecommunications links are often made to public databases and the information superhighway, so that external data can be browsed and incorporated into the models. While executive will frequently start with high-level summary data, if detail is required, there is the opportunity to `drill down' to the appropriate level and examine what makes up the summary.

EXPERT SYSTEMS:

- These are designed to replace the need for a human expert.
- They are particularly important where expertise is scarce and therefore expensive.
- This is not `number-crunching' software, but software that expresses knowledge in terms of facts and rules.
- The knowledge of these systems will be in a specific area, and therefore expert systems are not general. Ex an expert system for oil drilling is not much use in solving company taxation problems.

While there may have been a progression from transaction-processing systems, through management information systems, to decision-support and executive information systems, expert systems have arisen largely from academic research into artificial intelligence. The expert systems should be able to learn, i.e. change or add new rules. They are developed using very different programming languages such as PROLOG, which are referred to as fifth generation languages.

CHAPTER 2

TRANSACTION PROCESSING SYSTEM

INTRODUCTION

Transaction processing systems (TPS) are the basic business systems that process day-to-day transactions of an organization to carry on its business operations. It can be defined as:

"Transaction processing systems are computerized systems that perform and record the daily routine transactions necessary to conduct the business".

Transaction processing systems depend heavily on the flow of data through various organizational subsystems. It is important to manage, control, and speed this movement of data. As transaction data flow through various organisational channels, the data might be lost, inaccurately copied, delayed, or misinterpreted. Effective transaction processing systems ensure the capture of appropriate data and accurate information reporting.

TRANSACTION PROCESSING CYCLE

Most business organisations have in common, transactions that may be grouped according to four common cycles of business activity.

- **Revenue cycle:** Events related to the distribution of goods and services to other entities and the collection of related payments.
- **Expenditure cycle:** Events related to the acquisition of goods and services from other entities and the settlement of related obligations.
- **Production cycle:** Events related to the transformation of resources into goods and services
- **Finance cycle:** Events related to the acquisition and management of capital funds, including cash.

A transaction processing cycle consists of one or more application systems. An Application system process logically related transactions. An organisation's revenue cycle might commonly include application systems involving customer order entry, billing, accounts receivable, and sales reporting. An expenditure cycle might commonly include application systems involving vendor selection and requisitioning, purchasing, accounts payable, and payroll. A production cycle might include application systems involving production control and reporting, product costing, inventory control, and properly accounting. An organization's finance cycle might include application systems concerned with cash management and control, debt management, and the administration of employee benefit plans.

The transaction cycle model of an organization includes a fifth cycle—the financial reporting cycle. The financial reporting cycle is not an operating cycle. It obtains accounting and operating data from the other cycles and processes these data in such a manner that financial reports may be prepared.

COMPONENTS OF A TRANSACTION PROCESSING SYSTEM

The principle components of a transaction processing system include inputs, processing, storage, and outputs. These components or elements are part of both manual and computerized systems.

Input: Source documents, such as customer orders, sales slips, invoices, purchase orders, and employee time cards, are the physical evidence of inputs into the transaction processing system.

They serve several purposes:

- Capture data
- Facilitate operations by communicating data and authorising another operation in the process

- Standardize operations by indicating what data require recording and what actions need to be taken.
- Provide a permanent file for future analysis, if the documents are retained.

Processing: Processing involves the use of journals and registers to provide a permanent and chronological record of inputs. The entries are done either by hand in simple manual systems or by a data entry operator using a PC.

Computer processing: When computers are used for processing, two different modes of processing accounting transactions are possible. These modes are *batch processing* and *direct processing*. Batch processing is conceptually very similar to a traditional manual accounting system. Batches of transactions are accumulated as a transaction file. Transaction files are printed to provide documentation of inputs to the accounting system. Transaction files are subsequently posted to ledgers by computer programs. The ledgers are then periodically processed to generate financial statements. The flow of processing in a batch processing computer system is essentially same as in traditional manual system-source documents to journals journal to ledgers, and ledgers to financial statements.

In direct processing, individual transactions are posted directly to ledgers rather than being batched to build a transaction file. A ledger may be periodically processed to generate a listing of transactions that have been posted to it over some period of time. But this transaction file is created as a by-product of posting the ledger. Ledgers are periodically processed to generate financial statements.

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. They provide a summary of a firm's financial accounting transactions. All accounting transactions must be reflected in the general ledger. A debit-credit entry is input for every transaction. Traditionally, this process has been called posting. The general ledger generates a trial balance to test the accuracy of the entire prior record keeping.

Computer storage: In a computerized environment the storage takes place in the form of files on the various storage media. A file is an organized collection of data. There are several types of files. A **transaction file** is a collection of transactions data. Transaction files usually contain data that are temporary rather than permanent interest. By contrast, a **master file** contains data that are of a more permanent or continuing interest.

A **reference or table file** contains data that are necessary to support data processing. Common examples of reference files used in data processing are payroll tax tables and master price lists.

Outputs: There are a wide variety of outputs from a transaction processing system. Any document generated in the system is an output. Some documents are both output and input for e.g., a customer invoice is an output from the order-entry application system and also an input document to the accounts receivable application. Other common outputs of a transaction processing system are the trial balance, financial reports, operational reports, pay cheques, bills of lading, and vouchers.

The trail balance lists the balances of all the accounts in the general ledger and tests the accuracy of the record keeping. Thus, it is fundamental to financial control and preparation of financial statements.

CHAPTER 3

BASIC CONCEPTS OF MIS

INTRODUCTION

Management information system, or MIS, as it is popularly known, is an old management tool. It is being used by business managers as a means for better management and scientific decision-making. However, it has attained new dimensions after the advent of computers. The computer has helped in accurate processing of increased volumes of data at high speed, thereby, permitting the consideration of more alternatives in decision making process. Thus, the managers can extend their basic decision-making and communication skills with computer usage to increase their productivity and performance level.

CONCEPT OF MIS

What is MIS? MIS consists of three terms i.e., management, information and system. The concept of MIS is better understood if each element of term MIS is defined separately.

Management
Information
System

Management information system

Management:

- Management comprises the processes or activities that describe what managers do in the operation of their organization: plan, organize, initiate, and control operations.
- Management refers to a set of functions and process 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.
- It involves mobilization, combination, allocation and utilization of physical human and other needed resources in a judicious manner by employing appropriate skills, approaches and techniques.

Information:

Information is data that have been put into a meaningful and useful form. It has been defined as- "information is data that has been processed into a form that is meaningful to the recipient". For example, data regarding sales by various salesmen can be merged to provide information regarding total sales. This information is of vital importance to a marketing manager who is trying to plan for future sales.

The management plays the part of converting the information into action through the familiar process of decision-making. Information has come to occupy a very important position in the survival of a business.

System:

System may be defined as a composite entity consisting of a number of elements, which are interdependent and interacting, operating together for the accomplishment of an objective. A business is also a system where economic resources such as people, money, material, machines, etc. are transformed by various organization processes (such as production, marketing, finance, etc) into goods and services.

Definition of MIS: "An approach that visualize 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 the optimization of overall enterprise goals".

CHARACTERISTICS OF AN EFFECTIVE MIS: Important characteristics for an effective MIS are eight in number and are briefly discussed below:

1. *Management oriented:* It means that effort for the development of the information system should start from an appraisal of management needs and overall business objectives. Such a system is not necessarily for top management only, it may also meet the information requirements of middle level or operating levels management as well.
2. *Management directed:* Because of management orientation of MIS, it is necessary that management should actively direct the system's development efforts. Mere one time involvement is not enough. For system's effectiveness, it is necessary for management to devote their sufficient time not only at the stage of designing the system but for its review as well, to ensure that the implemented system meets the specification of the designed system.
3. *Integrated:* Development of information system should be an integrated one. It means that all the functional and operational information sub-systems should be tied together into one entity. An integrated information system has the capability of generating more meaningful information to management.
4. *Common data flows:* It means the use of common input, processing and output procedures and media whenever possible is desirable. Data is captured by system analysts only once and as close to its original source as possible. This eliminates duplication in data collections, documents and procedures. It also simplifies operations and produces an efficient information.
5. *Heavy planning element:* An MIS usually takes 3 to 5 years and sometimes even longer period to get established firmly with a company. Therefore, a heavy planning element must be present in MIS development. It means that MIS designer should keep in view future objectives and requirements of firm's information in mind. The designer must avoid the possibility of system obsolescence before the system gets into operation.
6. *Sub system concept:* Even though the information system is viewed as a single entity, it must be broken down into digestible sub-systems which can be implemented one at a time by developing a phasing plan.
7. *Common database:* It is defined as a "super file" which consolidates and integrates data records formerly stored in many separate data files. The organization of a database allows it to be accessed by several information sub-systems and thus, eliminates the necessity of duplication in data storage, updating, deletion and protection.
8. *Computerized:* It is possible to have MIS without using a computer. But use of computers increases the effectiveness of the system. In fact, its use equips the system to handle a wide variety of applications by providing their information requirements quickly. Other necessary attributes of the computer to MIS are accuracy and consistency in processing data and reduction in clerical staff. These attributes make computer a prime requirement in management information system.

Misconceptions or Myths about MIS:

Let us clarify some of the misconceptions or "myths" about MIS

1. *The study of management information system is about the use of computers:* This statement is not true. MIS may not be computer based, computer is just a tool, just like any other machine. Installing computer in an MIS depends largely on several factors such as, how critical is the response time required for getting an information; how big is the organization, and how complex are the needs of the information processing.
2. *More data in reports means more information for managers:* This is a misinterpretation. It is not quantity of data, but its relevance, which is important to mangers in process of decision-making. Data provided in reports should meet information requirements of mangers.
3. *Accuracy in reporting is of vital importance:* The popular belief is that accuracy in reporting should be of high order. At the operating level, it is true. Higher levels of accuracy involve higher cost. At higher decision levels, great accuracy may not be required. The degree of accuracy is closely related to the decision problem. Higher management is concerned with broad decisions on principles and objectives. A fairly correct presentation of relevant data often is adequate for top management decisions.

Pre-requisites of an effective MIS:

The main pre-requisites of an effective MIS are as follows:

(a) DataBase: It can be defined as a "superfile" which consolidates data records formerly stored in many data files. The data in database is organized in such a way that access to the data is improved and redundancy is reduced. Normally, the database is subdivided into the major information sub-sets needed to run a business. These sub-sets are (a) customer and Sale File; (b) vendor file; (e) Personal file; (d) Inventory file; and (e) General Ledger Accounting file. The main characteristic of database is that each sub-system utilizes same data and information kept in the same file to satisfy its information needs. The other important characteristics of data base are as follows:

1. It is users oriented.
2. It is capable of being used as a common data source, to various users, helps in avoiding duplication of efforts in storage and retrieval of data and information.
3. It is available to authorized persons only.
4. A separate authority established for the purpose, known as Data Base Management System (DBMS) controls it.

The maintenance of database requires computer hardware, software and experienced computer professionals, in addition it requires a good data collection system equipped with experts who have first-hand knowledge of the operations of the company and its information needs.

The database structured on above lines is capable of meeting information requirements of its executives, which is necessary for planning organizing and controlling the operations of the business concern.

(b) *Qualified system and management staff:* The second pre-requisite of effective MIS is that it should be manned by qualified officers. For this, the organizational management base should comprise of two categories of officers viz. (1) Systems and computer experts and (2) Management experts.

Systems and Computer experts in addition to their expertise in their subject area should also be capable of understanding management concepts to facilitate the understanding of problems faced by the concern. They should also be clear about the process of decision making and information requirements for planning and control functions.

Management experts should also understand quite clearly the concepts and operations of a computer. This basic knowledge of computers will be useful to place them in a comfortable position, while working with systems technicians in designing or other wise of the information system.

(c) *Support of Top Management:* The management information system to be effective, should receive the full support of top management. To gain the support of top management, the officers should place before top management all the supporting facts and state clearly the benefits which will accrue from it to the concern.

(d) *Control and maintenance of MIS:* Control of the MIS means the operation of the system as it was designed to operate. Some time, users develop their own procedures or short cut methods to use the system which reduce its effectiveness. To check such habits of users, the management at each level in the organization should devise checks for the information system control.

Maintenance is closely related to control. There are times when the need for improvements to the system will be discovered. Formal methods for changing and documenting changes must be provided.

(e) Evaluation of MIS: An effective MIS should be capable of meeting the information requirements of its executives in future as well. This capability can be maintained by evaluating the MIS and

taking appropriate timely action. The evaluation of MIS should take into account the following points.

1. Examining whether enough flexibility exists in the system, to cope with any expected or unexpected information requirement in future.
2. Ascertaining the view of users and the designers about the capabilities and deficiencies of the system.
3. Guiding the appropriate authority about the steps to be taken to maintain effectiveness of MIS.

Constraints in operating a MIS:

Major constraints that come in the way of operating an information system are the following:

1. *Non-availability of experts*, who can diagnose the objectives of the organization and provide a desired direction for installing and operating the system.
   This problem may be overcome by grooming internal staff. The grooming of staff should be preceded by proper selection and training.
2. Experts usually face the problem of selecting the sub-system of MIS to be installed and operated upon.
   However, they can decide the sub-system to be developed first based on the need and importance of the function.
3. Due to varied objectives of business concerns, the approach adopted by experts for designing and implementing MIS is a non-standard one.
   Though in this regard nothing can be done at the initial stage but by and by standardization may be arrived at, for the organization in the same industry.
4. Non-availability of cooperation from staff in fact is a crucial problem.
   This problem may be solved by educating the staff. This task should be carried out by organizing lecturers, showing films and also explaining to them the utility of the system. Besides this, some persons should also be involved in the development and implementation of the system.
5. There is high turnover of experts in MIS. Turnover in fact arises due to several factors like pay packet; promotion chances; future prospects, behavior of top ranking managers etc.
   Turnover of experts can be reduced by creating better working conditions and paying at least at par with other similar concerns.
6. Difficulty in quantifying the benefits of MIS, so that it can't be easily comparable with cost. This raises questions by departmental mangers about the utility of MIS.

Effects of using Computer for MIS:

The effect of applying computer technology to information system can be listed as below:

1. *Speed of processing and retrieval of data increases:* Modern business situations are characterized by high degree of complexity, keen competition and high risk and reward factors. This invariably calls for systems capable for providing relevant information with minimum loss of time. Manual systems often fail to match the demand for information for decision making. Computer with its unbelievably fast computational capability and systematic storage of information with random access facility has emerged as an answer to the problems faced in modern day management.
2. *Scope of use of information system has expanded:* The importance and utility of information system in business organizations was realized by most of the concerns, especially after the induction of computers for MIS development. Systems experts in business organizations developed areas and functions, where computerized MIS could be used to improve the working of the concern. These types of applications are not feasible under the manual system. For example, it was made possible by using an on line real time system to provide information to various users sitting at a remote distance from a centrally located computer systems.
3. *Scope of analysis widened:* The use of computer can provide multiple type of information accurately and in no time to decision-makers. Such information equips an executive to carry out a through analysis of the problems and to arrive at the final decision.

4. *Complexity of system design and operation increased:* The need for highly processed and sophisticated information based on multiple types of variables has made the designing of the system quite complex. During the initial years, after the induction of computer for MIS development, systems experts faced problems in designing systems and their operations. The reason at that time was the non-availability of experts required for the purpose. But these days the situation is better because computer manufacturers have developed some important programs (software) to help their users.
5. *Integrates the working of different information sub-system:* A suitable structure of management information system may be an association of information sub-system, viz., production, material, marketing, finance, engineering and personnel. Each of these sub-systems is required to provide information to support operational control, management control and strategic planning. Such information may be made available from a common database. This common database may meet out the information requirements of different information sub-system by utilising the services of computer. In this way, computer technology is useful for integrating the day-to-day working of different information sub system.
6. *Increases the effectiveness of Information system:* Information received in time is of immense value and importance to a concern. Prior to the use of computer technology for information purposes, it was difficult to provide the relevant information to business executives in time even after incurring huge expenses. The use of computer technology has overcome this problem. Now, it is not difficult to provide timely, accurate and desired information for the purpose of decision making. Hence, we can conclude that the use of computer has increased the effectiveness of information system also.
7. *More comprehensive information:* The use of computer for MIS enabled systems experts to provide more comprehensive information to executives on business matters.

Limitations of MIS: The main limitations of MIS are as follows:

1. The quality of the outputs of MIS is basically governed by the quantity of input and processes.
2. MIS is not substitute for effective management. It means that it cannot replace managerial judgement in making decisions in different functional areas. It is merely an important tool in the hands of executives for decision making and problem solving.
3. MIS may not have requisite flexibility to quickly update itself with the changing needs of time, especially in fast changing and complex environment.
4. MIS cannot provide tailor-made information packages suitable for the purpose of every type of decision made by executives.
5. MIS takes into account mainly quantitative factors, thus it ignores the non-quantitative factors like morale and attitude of members of the organization, which have an important bearing on the decision making process of executives.
6. MIS is less useful for making non-programmed decisions. Such types of decisions are not of the routine type and thus require extensive information, which may not be available from existing MIS to executives.
7. The effectiveness of MIS is reduced in organizations, where the culture of holding information and not sharing with other holds.
8. MIS effectiveness decreases due to frequent changes in top management, organizational structure and operational team.

INFORMATION NEEDS OF MANAGERS

Information is the substance on which business decisions are based. Therefore, the quality of data determines the quality of output i.e., information. This phenomenon is also known as garbage in garbage out (GIGO). The management plays the part of converting the information into actions through the familiar management process of decision making.

Establishing the information needs in management process:

In general the planning information requirements of executives can be categorised into three broad categories viz.

(a) environmental
(b) competitive and
(c) internal.

(a) **Environment information:** It comprises of the following:

1. *Government policies:* Information about concessions/benefits, government policies in respect of tax concessions or any other aspects, which may be useful to the organization in the future period.
2. *Factors of production:* Information related with source, cost, location, availability accessibility and productivity are the major factors of production viz., (1) labor, (2) materials and parts and (3) capital.
3. *Technological environment:* Forecast of any technical changes in the industry and the probable effect of it on the firm.
4. *Economic trends:* It includes information relating to economic indicators like consumer disposal income, employment, productivity, capital investment etc.

(b) **Competitive information:** It includes the following:

1. *Industry demand:* Demand forecast of the industry in respect of the product manufactured and in the area in which the firm would be operating.
2. *Firm demand:* Assessment of the firm's product demand in the specified market. It also includes an assessment of firm's capability to meet firm's demand.
3. *The competitive data:* Data of competing firms for forecasting demand and making decisions and plans to achieve the forecast.

(c) ***Internal information:*** Usually includes information concerning organizations (1) sales forecast, (2) financial plan/budget, (3) supply factors, and (4) policies, which are vital for subsidiary planning at all levels in the organization.

Factors on which information requirements depend: The factors on which information requirements of executives depend are:

1. Operational function.
2. Type of decision making.
3. Level of management activity.

1. *Operational function:* The grouping of several functional units on the basis of related activities into a sub-system is termed as operational function. For example, in a business enterprise, marketing is an operational function, as it is the grouping of several functional units like market research, advertising, sales analysis and so on. Likewise, production finance, personnel etc. can all be considered as operational functions.

   Information requirements depend upon operational function. The information requirements of different operational functions vary not only in content but also in characteristics. In fact, the content of information depends upon the activities performed under an operational function.

2. Type of decision making: Organizational decisions can be categorized as programmed and non-programmed ones.

   Programmed decisions:
   - Programmed decisions refer to decisions made on problems and situations by reference to a predetermined set of previous cases, procedures, techniques and rules.
   - These are well-structured in advance and tested.

- As a problem or issue for decision making emerges, the relevant pre-decided rule or procedure is applied to arrive at the decision.
- Not much judgment is needed in finding solutions to such problems.
- It is a matter of identifying the problem and applying the rule.
- Decision making is thus simplified.
- One characteristic of programmed decisions is that they tend to be consistent over situations and time.
- Programmed decisions do not always mean solutions to simple problems.
- Decision-making could be programmed even to complex problems.

Non-programmed decisions:

- Non-programmed decisions are made on situations and problems, which are new and non-repetitive.
- The knowledge and information available for such decisions is very limited.
- They are non-programmed in the sense that they are not made by reference to any pre-determined procedures and rules but by application of managerial intelligence, experience and judgement.
- There is no simple or single best way of making decisions on unstructured problems.
- Solutions and decisions on these problems tend to be unique or unusual.

It is true that several decisions are neither completely programmed nor completely non-programmed but share the features of both.

3. *Level of management activity:* Different levels of management activities in management planning and control hierarchy are-strategic level, tactical level and operational level.

Strategic level:

- Strategic level management is concerned with developing of organizational mission, objectives and strategies.
- Decisions made at this level of organization to handle problems critical to the survival and success of the organization.
- They have a vital impact on the direction and functioning of the organization-as for example introduction of new products, making major new fund-raising and investment operations, adoption of new technology, and acquisition of outside enterprises and so on.
- Much analysis and judgement go into making strategic decisions.
- In a way, strategic decisions are comparable to non-programmed decisions and they share some of their characteristics.

Tactical level:

- Tactical level lies in middle of managerial hierarchy. At this level, managers plan, organize, lead and control the activities of other managers.
- Decisions made at this level called the tactical decisions (which are also called operational decisions) are made to implement strategic decisions.
- A single strategic decision calls for a series of tactical decisions, which are of a relatively structured nature.
- Tactical decisions are relatively short step-like spot solutions to breakdown strategic decisions into implementable packages.

Supervisory level:

- This is the lowest level in managerial hierarchy.
- The managers at this level coordinate the work of other who are not themselves managers.
- They ensure that specific tasks are carried out effectively and efficiently.

Levels of management and their information requirements: There is no unanimity over the number of management levels. Different people classified the management in different levels in which, one common classification is as top level, middle level and supervisory level. The division of management into three levels is carried out to distinguish the type of tasks, extent of authority and degree of accountability within the hierarchy.

Top level (strategic level): Top management is defined as a set of management positions which are concerned with the overall task designing, directing and managing the organization in an integrated manner.

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 and broad objectives of the company. Also, it establishes a budget framework under which the various departments will operate.

- Top management needs information on the trends in the external environment (economic, technological, political and social) and on the functioning of the internal organizational sub-system.
- Apart from historical information, top management requires ongoing or current information also, which is generated through forecasts of the future.
- Mostly the information utilized by top management is futuristic and external in nature.
- Much of the information so generated for strategic planning purpose tends to be incomplete and not fully reliable.
- It may not be available on time.

  Ex: External: Customer preferences about products or services, Competitive Activities, Technological changes etc.

  Internal: Historical-sales and costs, Financial ratios, interests, credit outstanding, long-term debt, delinquent accounts etc.

Middle Level (Tactical level): Middle management is defined as a group of management position, which tends to overlap the top and supervisory management levels in the hierarchy. Middle management positions consist of heads of functional departments and chiefs of technical staff and service units. Middle management, therefore, includes such people as the manager of sales, the manager of purchasing, finance manger, and the manager of personnel etc.

- The nature of information required at the middle management level is less diverse and complex.
- Middle management is fed with information both from top management and supervisory management.
- Much of the information used by the middle management is internal in nature.
- Middle management does not require much 'futuristic' information since its decision are not strategic or long range in nature.

  Ex:

  External: Price changes, shortages, demand or supply, credit conditions etc.

  Internal: Current performance indicators, Over-under budgets etc.

Supervisory level: Supervisory management is defined as a team of management positions at the base of the hierarchy. It consists of section officers, office managers and Superintendents, Foreman and supervisors who are directly responsible for instructing and supervising the efforts of clerical and 'blue collar' employees and workers. Supervisory management is also called 'operations management' in the sense that it is concerned with implementing operational plans, policies and procedures for purpose of conversion of inputs into outputs. At the supervisory level, managers are responsible for routine, day-to-day decisions and activities of the organization which do not require much judgement and discretion.

- Supervisory management mostly needs internal information on operational aspects of the functioning of activity units.
- It also receives information from the middle management levels on operational plans and programs.
- The nature of information is routine and structured.
- It tends to be reliable and relatively complete.
- There is little element of complexity or uncertainly involved in the information.
  Ex:
  External: Changes in material supplies and sales etc.
  Internal: Unit sales and expenses, shortage and bottle necks etc.

CHAPTER 4

SYSTEMS APPROACH AND DECISION MAKING

SYSTEMS APPROACH TO MANAGEMENT PROBLEM SOLVING:

The systems approach to management is in fact a way of thinking about management problems. It visualizes an organisation as a group of interacting and interdependent parts with a purpose. Managers are not in a position to deal with individual parts separately since action of one part is going to influence other parts. Before solving the problem in any functional area, or in any specific sector of the organisation, the manager should understand fully how the overall system would respond to changes in its component parts.

How the system approach to problem solving is applied can be easily understood by the following steps.

1. Defining of the problem.
2. Collecting and analysing data concerning the problem.
3. Identification of alternate solutions.
4. Evaluation of alternative solutions.
5. Selection of the best alternative.
6. Implementation of the solution.

DECISION MAKING IN MIS:

Meaning and Nature of Decision Making:

In the context of organisation and Management, we may define 'decision making as a managerial process and function of choosing a particular alternative from a set of several alternatives for the purpose of achieving the given goals'. In a sense, decision-making is an important step towards reducing the gap between present situation and the desired situation.

Most of the managerial decisions are directed towards making the organisation survive, succeed and grow. Some times managers have to take painful decisions for example, removal of an employee or officer, withdrawal of products from the market, closing down certain units etc. Also, several decisions have to be made within a limited time, managers are hard pressed even they may not able wait for collection and analyses of complete information. These are crisis decisions.

Decision-making is one of the most important managerial functions. Managers manage by making decision and getting them implemented in systematic manner. Top managers make all the organisational decisions. However, it is the responsibility of the top management to create a decision-making system as an integral part of the organisational system. Such decision-making system is created through proper delegation of authority, installation of a suitable information system, and training of subordinate managers to improve their decision-making, creation of an organisational climate for making sound decisions.

Classification of Decisions:

Managers make a variety of decisions in their day-to-day working life without really bothering much about what types of decisions these are. For a better understanding about the nature of decisions, they have been categorised as under:

-Programmed and Non-Programmed decisions
-Strategic and Tactical decisions.
-Individual and Group decisions.

Programmed Decisions:

As discussed in the previous chapter.

Strategic and Tactical Decisions:

Strategic Decisions:

- Strategic decisions are made at the strategic level management of organisation.
- These are the decisions to handle problems critical to the survival and success of the organisation.
- These have a vital impact on the direction and functioning of the organisation.
- Much analyses and judgment go into strategic decisions.
- In a way these are comparable to non-programmed decisions and they share some of their characteristics.

Tactical Decisions:

- Tactical decisions are the decisions made at middle level of management.
- These are also called operational decisions.
- These decisions are made to implement strategic decisions.
- These are usually structured in nature.
- These are more specific and functional; information for tactical decisions is more easily available.
- These involve less uncertainty and complexity.
- The decision variables can be easily forecasted and quantified without much difficulty.

Individual and Group Decisions:

Individual Decisions:

- Individual decisions are those which are made by an individual manager.
- Many decisions, even critical ones, in organisations are made by individual managers, who assume full responsibility for the consequences of such decisions.
- The individual managers at their respective levels right from the chief executive down to first line supervisor are called upon to decide many things.
- They may get information, analytical reports, pros and cons of alternatives and suggested courses of action from their subordinates or from specially established committees, but the responsibility and authority of making final decision rests with the concerned manager himself.

Group Decisions:

- Group decisions are those which are made by more than one manager joining together for the purpose.
- In an organisation two or more managers at the same or different levels put their heads together, jointly deliberate on the problem, for which they assume collective responsibility.
- Decisions which have interdepartmental effects are some times made by forming a committee composed of responsible executives of the concern departments.
- Some times, group involvement in decision-making process may be confined to a few stages like problem identification, collection of information, development of alternative courses of action and their evaluation.
- The final act of choosing from the alternatives may be reserved by the manager concerned. To this extent, group decision-making is different from group participating in decision-making.

The disadvantages of group decision-making are

-delay in decision-making,
-lack of responsibility among group members,
-dilution of the quality of decision by compromise among members of the group and so on.

DECISION MAKING THROUGH MIS: (Computerized Models)

A growing number of companies are making affective use of MIS and computerized models in the decision making process. Before developing a model, the activities, operations and information requirements of the concerned area are studied first. Such models allow a decision-maker to consider a large number of factors in decision-making process, which was not possible in manual system.

A computerized model may be created for accounting, production, and transportation manufacturing and marketing operations of the company. This type of models puts pertinent information into an analytical framework that aids the management decision-making process. Some of the benefits offered by this model are listed below.

- Makes a fairly accurate forecast of net income for one year.
- Prepares short-term profit plans and long-range projections.
- Provides preplanning information in budget preparation.
- Calculates variances between budgeted and actual results.
- Provides revised forecasts if not proceeding in accordance with plan.
- Acts as early warning system for monitoring activities and providing reactive plans.

Although the effect of computerized information systems on top management has been relatively limited, their use is rising.

FUNCTIONAL INFORMATION SYSTEM

There are various users of information systems in business as there are number of activities to be performed in order to solve business problems. Functional information system is a system developed for a specific functional area in the business system. Information systems are typical integration of functional information systems. The following are the four major functional information areas:

- Finance & Accounting.
- Production.
- Marketing.
- Personnel.

Finance & Accounting:

Finance and accounting are separate functions but are sufficiently related to be described together.

Financial decision-making:

Financial decision-making deals with procurement of funds and their effective utilisation in the business. Thus there are two important aspects of financial decision-making.

-Regarding procurement of funds and
-Regarding effective utilisation of funds.

Procurement of funds is a complicated problem as there are number of sources from where the funds may be procured. Funds may be raised from various long-term sources such as equity, debentures, bonds etc., or various short-term sources such as banks, suppliers, credit etc. These sources have different characteristics in terms of risk, control and cost.

The next set of financial decisions relate to effective utilisation of funds. There are several long term and short-term assets where funds are to be deployed. If the funds are not utilised in a manner so that they generate incremental income over their cost, there is no point in running the business. Thus, each decision should be properly analysed while investing in fixed assets. Similarly, investment in current assets should be properly monitored.

Financial Decisions:

Various financial decisions made with the help of financial information system are as follows:

1. Estimation of requirement of funds: A careful estimation of funds and the timing when they will be required is to be made. This can be done by forecasting all physical activities of the firm and translating them into monetary units.

2. Capital Structure Decision: Decisions are to be made to select an optimum mix of different sources of capital structure. There are various options available for procuring funds. Decision maker has to decide the ratio between debt & equity, long term and short term funds etc., he has to ensure that overall capital structure is such that the company is able to procure funds at optimum cost.
3. Capital Budgeting Decisions: Funds procured from various sources are required to be invested in different assets. With the help of capital budgeting the decision-maker can determine feasibility of investment in long-term assets.
4. Profit planning: Financial decision concerning profits and dividends are to be taken by decision-maker. He has to ensure adequate surpluses in future for growth and distribution of dividends.
5. Tax planning: Tax planning is aimed at reducing of outflow of cash by way of taxes so that the same can be effectively utilised for the benefit of business. The purpose of tax planning is to take full advantage of exemptions, deductions, concessions and other relieves.
6. Working Capital Management: Working Capital is concerned with investment of long-term funds into current assets. Decisions are to be taken for effective financing of current assets required for day-to-day running of the organisation.
7. Current asset Management: Policy decisions are taken regarding various items of current assets.

MARKETING SYSTEM

The marketing system is aimed at supporting the decision making, reporting and transaction processing requirements of marketing and Sales Management. The main objective of marketing management system is to develop, promote, distribute, sell and service the products of the organisation. To achieve this objective, marketing management needs information to make effective decision-making. Marketing bridges the gap between business firms and its customers, by making available the products of the business to the customers. The information that marketing management receives is important, however the information that marketing generates is vital to the rest of the orgnisation. For example, marketing provides sales forecasts that serve as the basis for production schedules, cash flow projections, and profit plans. So, the marketing information system in organisation must be designed in an effective way to support the marketing management in the organisation.

The marketing information system consists of the following subsystems in order to enhance the decisional capacities in various marketing activities.

1. Sales
2. Market Research & Intelligence
3. Advertising and promotion
4. Product development and planning
5. Product pricing system
6. Customer service

1. Sales:

The objective of the sales manager is to coordinate the sales effort so that the long-run profitability of the company is maximized. Decisions are required in the area of adequate stocks, effective distribution channels, effective motivation of sales personal, and good customer relations. The sales management requires the information for sales supports and Sales analysis.

(a)Sales Support:

The marketing information system, directly or indirectly support selling activity. However, a specialised sales support information system must provide information to sales personnel about the following.

- Product descriptions and performance specifications.
- Product prices.
- Quantity discounts and other product discount information.

- Sales promotions.
- The strengths and weaknesses of competitor's products.
- Sales policies and procedures established by the company and products inventory levels.

(b)Sales Analysis:
The sales analysis is a major activity in most companies involved in sales. Its purpose is to provide information for analyses of

- Product sales trend
- Product profitability
- The performance of each sales region and sales branch and
- The performance of the respective sales persons.

2. Market Research and Intelligence
The major objective of market research is to investigate problems confronting the other managers in the marketing function.

To satisfy the needs, the market research department gathers the information from a wide variety of sources. One major source is the sales system and other sources are outside the organisation. Marketing research will gather new information which will helps in managerial decision making. It investigates past, present and future states of the market place. The investigations undertaken by market research help in satisfaction of following informational needs of managers.

- Information about the economy and economic trends and the probable impact of these trends on demand for the product.
- Information about the past sales and sales trends for the entire industry.
- Information about the potential new markets for products.
- Information about competitors, its products, new product plans and so on.

The market research may be distinguished from market intelligence, the former concentrating on the market place and the later is concerned about only one aspect of the market place, i.e. the organisation's competitors. However the information required by the both functions come from same source.

3. Advertising and promotion:
The advertising and promotion development devotes its attention to plan and execute advertising campaign and to carry out various product promotions such as coupons, contests, trade shows and so on.

The promotion and advertising information system should store the house of information that managers can combine with their past experience for taking decision on promotion and advertising. By systematically organising and analysing this information, an organisation can establish a body of knowledge about what the market place is like and how it responds to each of several types of promotional activities for each product.

4. Product Development and Planning:
Product Development involves analysing a possible opportunity for a new product and evaluating preferred specifications and probable market success. A customer call reports system may helps in gathering information about new products needed in the market place.

During the analysis of new product feasibility, after a probable need has been identified, information from the sales analysis system about past sales of similar or related products may indicate the desirable characteristics for the new product. Also market research can be tailored to gather information about the size and structure of the market place for the product and the marketing intelligence information system may help to evaluate the market strength and profitability of similar products produced by competitors.

The product development department uses all this information to develop specifications for a new product. These specifications may then be passed along to engineering and other groups for cost estimating. Risk profiles, which include estimated costs and revenues for the product over its life cycle, are developed as a basis for deciding whether to produce the product or not.
Product planning system provides marketing management with packaging, promotion, pricing and style recommendations throughout the life of product.

5. Product Pricing System:
Product pricing is a complex managerial activity that is effected by product costs, customer demand, market psychology, competitors prices and various actions taken by competitors and so on. Market research into the strength of demand for each product in the market place is also useful for pricing purposes. The most important information that the pricing system expects is about competitor's prices for similar products.

6. Customer service:
The objective of marketing department is to satisfy customers with the product. To achieve this objective customer service management provides customers with technical assistance and product maintenance. Decisions are taken in the area of training of service personnel, capabilities of equipment and location facilities to serve customers.

Information Required by a Marketing System:
The information for the purpose of planning in the case of marketing system can be classified into three broad types.

Environment Information.
Competitive Information.
Internal Information.

1. Environment Information:
Environment Information required for developing a Marketing system includes following:

a) *Political and Governmental Considerations:* To forecast market plans, information regarding political stability at any level i.e. at centre or state, national or international plays a significant role. Political stability enables executives to guess quite accurately the policies of the government and thus it helps them to reduce the risk while formulating plans for future.
b) *Demographic and Social trends:* Information about demography, its composition and location is also useful to business organisations for planning its products, services or outputs.
c) *Economic trends:* This includes information related to the GNP level and trend disposal income of consumers, employment, price and wage levels and other economic indicators, which provide valuable planning information for those firms whose output is function of these important variables.

2. Competitive information:
Data relating to business operations of competing firms is quite useful for forecasting individual firm's product demand and making decisions and plans to achieve the forecast.

3. Internal Information:
The information available from internal source is more important than the external one as it affects the planning decisions at different levels in the organisation. The main sources of internal information are.

Sales forecast
Financial plan
Supply factors
Policies

a) *Sales forecast:* It provides information about firm's sales plan. It sets the framework on which most of the internal plans are dependent.
b) *Financial plan:* Such a plan provides useful information for a variety of sub-plans throughout the firm.
c) *Supply factors:* Manpower, capital, plant and equipment and other supply factors are vital to establish planning premises that provide constraints or boundaries within which planning takes place.
d) *Policies:* Basic policies remain unchanged in the short run; they provide constraints to planning in the same way as the supply factors.

In the case of marketing system, the information required for the purpose of control are information concerning the progress of the sales plan, quotas, territories, pricing etc. In other words the information required is meant to measure performance against the sales forecast.

PRODUCTION SYSTEM:
One of the major areas in any kind of enterprise is production and operations management. Generally the term production management refers to those activities, which are necessary to manufacture products. However, in many companies the area is broad enough to include such activities as purchasing, warehousing transportation and other activities from the procurement of the raw material through various operations until a product is available to the buyer.

The role of production in organisations is to provide a product that the market demands. This means:

1. Producing the quantity of goods needed by customers.
2. Maintaining the quality of the products established by product specifications and,
3. Producing products within the cost constraints imposed by the production control system.

The major sub-system in production system includes.
-Production planning
-Production scheduling and
-Materials requirement planning.

Production planning:
It means determining
What should be produced?
When it should be produced and
How it should be produced.
It is primarily the responsibility of plant manager, general foreman and various production department foremen to perform the task of production planning. But usually production-planning department perform the task of production planning on the basis of sales plan and materials plan etc.

The main activities of a production plan include the following.
1. Breaking up the job into various divisions and subdivisions leading to the listing of all the operations, which would be carried out.
2. Making drawings or processing patterns etc.
3. Drawing up the Bill of material and the schedule of dates on which the various materials will be required.
4. Listing the tools required and for which any special procurement is to be made.
5. Making trail runs to locate and remove possible snags.
6. Drawing up the route chart by which the task will be completed and listing the exact methods, tools, machines, materials etc. This will be required for completing each operation. This is technically called routing.
7. Drawing up a detailed timetable for the entire activity to be completed.
8. Dispatching and issuing instructions for the various activities to be taken up.

Production Control:

It includes the control of all the activities related to production department or shops. The following are the areas where the optimum attention is required for control.

Time standards.
Quality standards and
Cost standards.

Time standards are usually incorporated in the operations list and are controlled by the department foremen by coordinating the task of works and machines. Cost standards mainly considered to see that materials are properly used and not wasted. Quality control is exercised with the help of a separate quality control department. This function involves testing or inspecting completed items of production or defects in materials etc. Basic information requirements of production planning & control system:

Basic information requirements of production planning and control system are as follows.

1. Firm's policy with regard to production of various products.
2. Sales order, sales forecast, stock position.
3. Available labor force with their capabilities.
4. Standards of labor time, material, machine time etc.
5. Schedule of meeting the sales orders, region wise, territory wise etc,
6. Quality norms for materials to be used and for the finished products.
7. Break-up of the jobs and their resource requirements.

Production scheduling:

The information provided by master production scheduling is used for different purposes. The main objectives of production scheduling department are as follows:

1. To determine the stages of production in sequential and rational order.
2. To minimize the idle time on the part of the operators and equipment.
3. To assess the extent of need for subcontracting to outside parties.
4. To ensure that completion dates or target dates of completing the production plans are met fully.
5. To study alternative methods of performing the activities so that time taken to perform can be further reduced.

Materials requirement planning:

A major cause of production inefficiency is a lack of integrated production planning, production scheduling and production control information systems. One approach to improve production efficiency is Materials Requirements Planning (MRP), its purpose is to greatly improve both inventory management and production scheduling.

The benefits of a successful MRP system include:

1. Significantly decreased inventory levels and correspondingly decreases in inventory carrying costs.
2. Fewer stock shortage, which causes production interruptions, can be avoided.
3. Increased effectiveness of production supervisors and less production problems.
4. Better customer service.
5. Greater responsiveness to change.
6. Closer coordination of the marketing, engineering and finance activities with the manufacturing activities.

PERSONNEL SYSTEM:

The personnel information system deals with the flow of information about people working in the organisation as well as future personnel needs. In most of the organisations, the system is concerned primarily with the six basic sub-systems of the personnel function:

-Recruitment
-Placement
-Training & Development
-Compensation
-Maintenance and
-Health & Safety.

Recruitment:
Properly managed recruitment sub-system may forecast personnel needs and skills required for recruiting personnel at the proper time to meet organisational manpower needs. Such a sub-system not only furnish the information concerning skills required for the company programs but also maintains the inventory of skills available within the organisation.

Placement:
This sub-system is concerned with the task of matching the available persons with the requirements.

Training & Development:
As technological changes and demands for new skills occurs, many companies find that they must develop much of their requirements from internal sources. This task is the function of the Training & Development sub-system.

Compensation:
This sub-system is concerned with the task of determining pay and other benefits for the workers of the concern. By considering government reports, union expectation etc. before arriving at the final figure of pay and other benefits for each category of workers.

Maintenance:
This sub-system is designed to ensure that personnel policies and procedures are achieved.

Health & Safety:
This sub-system is concerned with the health of personnel and safety of jobs in the organisation.

Sources of personnel Information system:
The Accounting Information System:
Bulk of the personnel information is generated by accounting department and with in the personnel department itself. Payroll processing is the traditional channel of personnel information. The human accounting and cost estimation for wage negotiation is another accounting information for the personnel function.

The personnel department itself generates a great deal of information in the form of personnel files and job specifications. Personnel files include such data about each employee as below.

- Physical characteristics
- Educational background and experience
- Pay roll information
- Quantitative and qualitative evaluations of his past performance.
- State of health and medical history.

Such information is quite useful for placement of employees for various positions promotions etc.

Other information generated within the personnel department may include forecasts of manpower requirements, records and statistics of training programs etc.

Payroll processing:

The inputs to payroll processing are the job tickets and the clock cards. The clock card indicates that the total number of hours an employee spends at work each day. This document serves as the basic input to the payroll calculation and pay slip preparation function. The job ticket is used to reconcile the timing on the clock card and various job statistics. The basic output of a payroll processing is pay slips and pay cheques. Other types of possible reports and analysis are listed below:

(a) Reports on absenteeism
(b) Analysis of individual labor
(c) Reports on actual standard costs
(d) Statistical measures as total number of employees, total hours worked, total labor cost, average wage rate, rate of absenteeism etc.

A part from internal generation, the personnel function also rely on external information sources. These would include employment agencies, labor unions, various governmental agencies, university placement offices etc.

CHAPTER 5

DECISION SUPPORT AND EXECUTIVE INFORMATION SYSTEMS

What is DSS?

A decision support system can be defined as a system that provides tools to managers to assist them in solving semi-structured and unstructured problems in their own. 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 the information required by them in making decisions. In other words, a DSS support the human decision making process, rather than providing a means to replace it.

The decision support systems are characterised by at least three properties:

1. They support semistructured or unstructured decision-making.
2. They are flexible enough to respond to the changing needs of decision makers, and
3. They are easy to use.

Semi-structured and Unstructured Decisions: Structured decisions are those that are easily made from a given set of inputs. These types of decisions—such as deciding to issue a reminder notice if a bill is overdue or deciding to sell a stock under a given set of market conditions-can be programmed fairly easily. Unstructured decisions and semistructured decisions, however, are decisions for which information obtained from a computer system is only a portion of the total knowledge needed to make the decision. The DSS is particularly well adapted to help with semistructured and unstructured decisions. However, it can be designed to support structured decision making as well. A manager, for instance, can browse through data at will. When enough information is gathered from this process to supplement other information a decision can be reached. In a well designed DSS, the depth to which the available data can be tapped for useful information often depends on the time availability and patience of the manager.

A semistructured problem might be solved by using a DSS. The problem is first defined and formulated. It is then modeled with DSS software. Next, the model is run on the computer to provide results. The modeler, in reviewing these results, might decide to completely reformulate the problem, refine the model, or use the model to obtain other results.

For example, a user might define a problem that involves simulating cash flows under a variety of business conditions by using financial modeling software. The DSS model is then run, providing results. Depending on what the results of the model indicate about cash flow, the user might decide to completely remodel the problem, make small modifications to the current model, run the model under a number of new assumptions, or accept the results.

Ability to adapt to changing needs: Semistructured and unstructured decisions often do not conform to a predefined set of decision-making rules. Because of this, the decision support systems must provide enough flexibility to enable users to model their own information needs. They should also be capable of adapting to changing information needs.

The DSS designer understands that managers usually do not know in advance what information they need and, even if they do that information needs keep changing constantly. Thus, rather than locking the system into rigid information producing requirements, capabilities and tools are provided by DSS to enable users to meet their own output needs.

Flexibility in a DSS is of paramount importance. Information requests made to a DSS will often be relatively unsystematic and distinctive. For example, a sales manager at a display device might request the price of a specific product. A few seconds later, the manager might change his mind and ask for a listing of the vendors of several other products. The next request, a couple of minutes later, may be a ranking of the top salespeople in a particular sales region over the last two months. A report might even be requested at the end of session, combining data from several of these inquiries.

Ease of learning and Use: Since decision support systems are often built and operated by users rather than by computer professionals, the tools that accompany them should be relatively easy to learn and use. Such software tools employ user-oriented interfaces such as grids, graphics, non-procedural fourth—generation languages (4GL), natural English, and easily read documentation. These interfaces make it easier for users to conceptualize and perform the decision-making process.

COMPONENTS OF A DSS

A decision support system has four basic components:

1. The user
2. One or more databases.
3. A planning language and
4. The modelbase.

1. The user: The users of a decision support system are usually a manager with an unstructured or semi-structured problem to solve. The manager may be at any level of authority in the organisation. Typically, users do not need a computer background to use a decision support system for problem solving. The most important knowledge is a thorough understanding of the problem and the factors to be considered in finding a solution. A user does not need extensive education in computer programming in part because a special planning language performs the communication function within the decision support system. Often, the planning language is nonprocedural, meaning that the user can concentrate on what should be accomplished rather than on how the computer should perform each step.

2. *Database:* Decision support systems include one or more databases. These databases contain both routine and non-routine data from both internal and external sources.

   The data from external sources include data about the operating environment surrounding an organisation for example, data about economic conditions, market demand for the organisation's goods or services, and industry competition. It also includes assumptions about such variables as interest rates, vacancy rates, market price, and levels of competition.

   Decision support system users may construct additional databases themselves. Some of the data may come from internal sources. An organisation often generates this type of data in the normal course of operations-for example, data from the financial and managerial accounting systems such as account, transaction and planning data. The database may also capture data from other subsystems such as marketing, production, and personnel.

3. Planning Languages: Two types planning languages that are commonly used in decision support systems are:

1. General purpose planning languages
2. Special purpose planning languages.

General purpose planning languages allow users to perform many routine tasks for example, retrieving various data from a database or performing statistical analyses. Electronic spreadsheets are good examples of general-purpose planning languages. These languages enable user to tackle a broad range of budgeting, forecasting and other worksheet oriented problems.

Special-purpose planning languages are more limited in what they can do, but they usually do certain special jobs better than the general-purpose planning languages.

4. Model base: The planning language in a decision support system allows the user to maintain a dialogue with the model base. The model base is the "brain" of the decision support system because it performs data manipulations and computations with the data provided to it by the user and the database. There are many types of model bases, but most of them are custom-developed models that do some types of mathematical functions-for example, cross tabulation, regression analysis, time

series analysis, linear programming and financial computations. The analysis provided by the routines in the model base is the key to support the user's decision.

THE TOOLS OF DECISION SUPPORT SYSTEMS

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

Database Languages: Tools supporting database query and report generation use mainframe, minicomputer, and microcomputer-based databases. FOCUS, RAMIS, and NOMAD II, for example, are mainframe-based languages supporting database query, report generation, and simple analysis. FOCUS and RAMIS are also available in PC versions. Ingress, Oracle, and Informix are database languages on mainframes, minicomputers, and microcomputers. Managers frequently use microcomputer-based database tools such as MS-Access dBase etc.

Decision support systems are widely used as part of an organization's AIS. The complexity and nature of decision support systems vary. Many are developed in-house using either a general type of decision support program or a spreadsheet program to solve specific problems.

Model-Base Decision Support Software: Model-based analysis tools such as spreadsheet software enable managers to design models that incorporate business rules and assumptions. Microcomputer-based spreadsheet programs such as Lotus and Excel all support model building and "What If?" types of analysis. Mainframe based spreadsheets such as Megacalc and Omnicalc fulfill the same purpose.

Tools for Statistics and Data Manipulation: Statistical analysis software such as SAS and SPSS supports market researchers, operations research analysts, and other professionals using statistical analysis functions. Because of the need for increased "number crunching" capabilities, this type of software usually runs on mainframe computers. Microcomputer-based statistical packages are available as well. For example the micro-based version of SPSS has about the same capabilities as the mainframe version, but it is much slower.

Display Based Decision Support Software: The final category of decision support software is display-based software. Graphics displays of output generated from MS-Excel spreadsheets, for example, are very effective in management presentations. Graphics tools running in a mainframe environment include DISSPLA, TELLGRAF, and SASGRAPH. Microcomputer-based tools such as Harvard Graphics and PowerPoint display graphics output in the form of variety of charts.

EXAMPLES OF DECISION SUPPORT SYSTEMS IN ACCOUNTING

Decision support systems are widely used as part of an orgnaisations AIS. The complexity and nature of decision support systems vary. Many are developed in-house using either a general type of decision support program or a spreadsheet program to solve specific problems. Following are some of the examples of these systems.

Cost Accounting system: The health care industry is well known for its cost complexity. Managing costs in this industry requires controlling costs of supplies, expensive machinery, technology, and a variety of personnel. Cost accounting applications help health care organizations calculate product costs for individual procedures or services. Decision support systems can accumulate these product costs to calculate total costs per patient. Health care managers may combine cost accounting decision support systems with other applications, such as productivity systems. Combining these applications allows managers to measure the effectiveness of specific operating processes. One health care organization, for example, combines a variety of decision support system applications in productivity, cost accounting, case mix, and nursing staff scheduling to improve its management decision making.

Capital Budgeting System: Companies require new tools to evaluate high-technology investment decisions. Decision-makers need to supplement analytical techniques, such as net present value and internal rate of return, with decision support tools that consider some benefits of new technology not captured in strict financial analysis. One decision support system designed to support decisions about investments in automated manufacturing technology is Automan, which allows decision makers to consider financial, non financial, quantitative, and qualitative factors in their decision-making process. Using this decision support system, accountants, managers, and engineers identify and prioritize these factors. They can then evaluate up to seven investment alternatives at once.

Budget Variance Analysis System: Financial institutions rely heavily on their budgeting systems for controlling costs and evaluating managerial performance. One institution uses a computerized decision support system to generate monthly variance reports for division controllers. The system allows these controllers to graph, view, budget projections using the forecasting tools provided in the system. The decision support system thus helps the controllers create and control budgets for the cost-center managers reporting to them.

General Decision Support System: As mentioned earlier, some planning languages used in decision support systems are general purpose and therefore have the ability to analyze many different types of problems. In a sense, these types of decision support systems are decision-maker's tools. An example is a program called **Expert Choice.** This program supports a variety of problems requiring decisions. The user works interactively with the computer to develop a hierarchical model of the decision problem. The decision support system then asks the user to compare decision variables with each other.

For instance, the system might ask the user how important can inflows are versus initial investment amount to a capital budgeting decision. The decision-maker also makes judgements about which investment is best with respect to this cash flow and which requires the smallest initial investment. Expert choice analyzes these judgements and presents the decision-maker with the best alternative.

EXECUTIVE INFORMATION SYSTEMS

An executive information system-which is sometimes referred to as an executive support system is designed to meet the special needs of top-level managers. Some people use the terms "EIS" and "ESS" interchangeably. Any distinction between the two usually is because executive support systems are likely to incorporate additional capabilities such as electronic mail.

In this section, we first cover those people in organizations that are considered to be executives and examine the types of decisions they make. Then, we will turn to the nature of executive decisions and the types of information that executives need most. Finally, some of the special characteristics of executive information systems—beyond those of other decision support systems—are discussed.

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 of action taken by the organization. The slots in a firm considered to be executive positions vary from company to company. For example, in many firms, the chief information officer is usually an executive who participates in key strategic decisions. In other firms, the CIO is a middle manager. And sometimes, the person in charge of an organisation's CBIS is basically a data processing director.

Executive Roles and Decision Making: Most executive decisions fall into one of three classes: strategic planning, tactical planning and "fire-fighting" activities and executives need a certain degree of control to ensure that these activities are carried out properly.

Strategic Planning: Strategic planning involves determining the general, long-range direction of the organization. Typically, the CEO is ultimately responsible for the development of strategic plans.

Tactical Planning: Whereas strategic planning addresses the general concerns of the firm, tactical planning refers to the how, when, where, and what issues involved with carrying out the strategic plan. Although executives will not normally be concerned with tactical details, they do need to worry about general tactics. For example, the vice president of finance must address how the firm can best achieve a balance between debt and equity financing. And the marketing vice-president will need to consider which classes of products the company should produce to be successful in the marketplace.

Fire Fighting: Major problems arise sometimes that must be resolved by someone at an executive level. For example, if a company is involved in a big lawsuit that threatens its financial solvency, an executive must get involved. Other possible fire-fighting activities include damage caused to a major facility, the announcement of an important product by a competitor, a strike, and a sharp reversal of the economy. Many of these events will call for key alterations in plans.

Control: In addition to planning and fire-fighting, executive management also needs to exercise some general control over the organization. Thus, executives will also periodically review key performance data to see how they compare against planned amounts.

The executive Decision-Making Environment: The three main sources for executive information are as follows:

1. Environmental information
2. Competitive information
3. Internal information

The type of decisions that executives must make is broad. Often, executives make these decisions based on a vision they have regarding what it will take to make their companies successful.

There are five characteristics of the types of information used in executive decision making are lack of structure, high degree of uncertainty, future orientation, informal source, and low level of detail. These are discussed below:

- **Lack of structure:** Many of the decisions made by executives are relatively unstructured. For instance, what general direction should the company take? Or what type of advertising campaign will best promote the new product line? These types of decisions are not as clear-cut as deciding how to debug a computer program or how to deal with an overdue account balance. Also, it is not always obvious which data are required or how to weigh available data when reaching a decision.

- **High degree of uncertainty:** Executives work in a decision space that is often characterized by lack of precedent. Executives also work in a decision space where results are not scientifically predictable from actions.

- **Future orientation:** Strategic-planning decisions are made in order to shape future events. As conditions change, organizations must change also. It is the executive's responsibility to make sure that the organization keeps pointed towards the future. Some key questions about the future include: "How will future technologies affect? What the company is currently doing? What will the competition (or the government) do next? What products will consumers demand five years from now? Where will the economy move next, and how might that affect consumer buying patterns?" As one can see, the answers to all of these questions about the future external environment are vital.

- **Informal source:** Executives, more than other types of managers, rely heavily on informal source for key information. For example, lunch with a colleague in another firm might reveal some important competitor strategies. Informal sources such television might also feature news of moment's concern to the executive news that he or she would probably never encounter in the company's database or scheduled computer reports. Besides business meals and the media, some

other important information sources of information are meetings, tours around the company's facilities to chat with employees, brainstorming with a trusted colleague or two, and social events.

- **Low level of detail:** Most important executive decisions are made by observing broad trends. This requires the executives to be more aware of the large overview than the tiny items. Even so, many executives insist that the answers to some questions can only be found by mucking through details.

EIS ROLES AND CHARACTERISTICS

Studies on EIS implementation show that thousands of companies have implemented executive information systems. Usually, the executive information systems provide executives with access to financial data, marketing and sales information, human resources information, manufacturing data, and competitive/strategic information. Electronic mail, access to external news and databases, word processing spreadsheet, and automated filing capabilities are also common in business executive information systems. While it is often expensive to develop and maintain an EIS, many organizations feel that enhanced top level decision making is a benefit that more than balances out any costs associated with the system.

Characteristics of an Executive Information System (EIS):

The EIS is a relatively recent development, which has evolved from earlier management information system (MIS). Its main characteristics are

- Screen-based-All EIS's are delivered through terminals using easy-to-use software.
- Mouse, icons and touch-screen facilities are usual.
- Information tends to be presented by pictorial or graphical means.
- Information is presented in summary format, eg: sales for the whole company. There is, however, the facility to `drill down' to other levels of information to see how the sales figure were arrived at-by geographical location, by product group etc.
- The ability to manipulate data, to project `what if' outcomes and to work with modeling tools within the system are also evident in EIS. This is particularly so with external information that can be `superimposed' onto the company's information.

WHAT IS AN EXECUTIVE INFORMATION SYSTEM?

An Executive Information System (EIS) is a tool that provides direct on-line access to relevant information in a useful and navigable format. Relevant information is timely, accurate, and actionable information about aspects of a business that are of particular interest to the senior manager. The useful and navigable format of the system means that it is specifically designed to be used by individuals with limited time, limited keyboarding skills, and little direct experience with computers.

An EIS differ from traditional information systems in the following ways:

- They are specifically tailored to executive's information needs.
- They are able to access data about specific issues and problems as well as aggregate reports.
- They provide extensive on-line analysis tools including trend analysis, exception reporting.
- They can access a broad range of internal and external data.
- They are particularly easy to use (typically mouse or touch-screen driven).
- They are used directly by executives without assistance.
- Screen-based-All EISs are delivered through terminals using easy-to-use software.
- Information tends to be presented by pictorial graphical means.
- Information is presented in summary format, e.g., sales for the whole company. There is, however, the facility to 'drill down' to other levels of information to see how the sale figure were arrived at-by geographical location, by product group etc. sales forecasts with information from the Meteorological Office about the weather.

Purpose of EIS: These are stated below:

1. The primary purpose of an Executive Information System is to support managerial learning about an organization, its work processes, and its interaction with the external environment. Informed managers can ask better questions and make better decisions.

2. A secondary purpose for an EIS is to allow timely access to information. All of the information contained in an EIS can typically be obtained by a manager through traditional methods. However, the resources and time required to manually compile information in a wide variety of formats, and in response to ever changing and ever more specific questions usually inhibit managers from obtaining this information. Often, by the time of useful report can be compiled, the strategic issues facing the manager have changed, and the report is never fully utilized.

   Timely access also influences learning. When a manager obtains the answer to a question, that answer typically sparks other related question in the manager's mind. If those questions can be posed immediately, and the next answer retrieved, the learning cycle continues unbroken. Using traditional methods, by the time the answer is produced, the context of the question may be lost, and the learning cycle will not continue.

3. A third purpose of an EIS is commonly misperceived. An EIS has a powerful ability to direct management attention to specific areas of the organization or specific business problems. Some managers see this as an opportunity to discipline subordinates. Some subordinates fear the directive nature of the system and spend a great deal of time trying to outwit or discredit it. Neither of these behaviors is appropriate or productive. Rather, managers and subordinates can work together to determine the root causes of issues highlighted by the EIS.

Contents of EIS: A general answer to the question of what data is appropriate for inclusion in an Executive Information System is "whatever is interesting to executives". Executive Information Systems in government have been constructed to track data about Ministerial correspondence, case management, worker productivity, finances, and human resources to name only a few. Other sectors use EIS implementations to monitor information about competitors in the news media and databases of public information in addition to the traditional revenue, cost, volume, sales, and market share and quality applications.

Frequently, 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. Overtime, the presentation of this information becomes old, and the information diverges from what is strategically important for the organization.

While the above indicates that selection of data for inclusion in an EIS is difficult, there are several guidelines that help to make that assessment. A practical set of principles to guide the design of measures and indicators to be included in an EIS is presented below.

1. EIS measures must be easy to understand and collect. Wherever possible, data should be collected naturally as part of the process of work. An EIS should not add work substantially to the workload of managers or staff.
2. EIS measures must be based on a balanced view of the organization's objective. Data in the system should reflect the objectives of the organization in the areas of productivity, resource management, and quality and customer service.
3. Performance indicators in an EIS must reflect everyone's contribution in a fair and consistent manner. Indicators should be as independent as possible from variables outside the control of managers.

4. EIS measures must encourage management and staff to share ownership of the organization's objectives. Performance indicators must promote both teamwork and friendly competition. Measures will be meaningful for all staff; people must feel that they, as individuals, can contribute to improving the performance of the organization.
5. EIS information must be available to everyone in the organization. The objective is to provide everyone with useful information about the organization's performance. Information that must remain confidential should not be part of the EIS or the management system of the organization.
6. EIS measures must evolve to meet the changing needs of the organization.

COMMERCIALLY AVAILABLE EIS PRODUCTS

Many EIS generators—EIS development packages-are commercially available. Commander EIS (from Comshare, Inc) Command Center (from Pilot Executive Software), Executive Edge (from Execucom Systems Corporation), and Express EIS (from Information Resources, Inc) are among the market leaders in the U.S. RESOLVE is another leading product, especially in Europe.

CHAPTER 6

ENABALING TECHNOLOGIES

CLIENT/SERVER ARCHITECTURE

Recently, many organisations have been adopting a form of distributed processing called client/server computing. It can be defined as "a form of shared or distributed computing in which tasks and computing power are split between servers and clients (usually workstations or personal computers)". Servers store and process data common to users across the enterprise, these data can then be accessed by client system. In this section we will discuss various aspects of client/server technology. But before that, let first look at the characteristics of the traditional computing models and various limitations that led to the client/server computing.

THE TRADITIONAL COMPUTING MODEL

1. *Mainframe architecture:* With mainframe software architectures, all intelligence is within the central host computer. Users interact with the host through a dump terminal that captures keystrokes and sends that information to the host. Centralized host based computing models allow many users to share a single computer's applications, databases, and peripherals.

   A limitation of mainframe software architectures is that they do not easily support graphical user interfaces or access to multiple databases from geographically dispersed sites. They cost literally thousands of times more than PCs, but they don't do thousands of times more work.

2. *Personal Computers:* With introduction of the PC and its operating system, independent-computing workstations quickly became common. Disconnected, independent personal computing models allow processing loads to be removed from a central computer. Besides not being able to share data, disconnected personal workstation users cannot share expensive resources that mainframe system users can share disk drives, printers, modems, and other peripheral computing devices. The data (and peripheral) sharing problems of independent PCs and workstations, quickly led to the birth of the network/file server computing model, which links PCs and workstations together in a Local Area Network-LAN, so they can share data and peripherals.

3. *File sharing architecture:* The original PC networks were based on file sharing architectures, where the server downloads files from the shared location to the desktop environment. The requested user job is then run in the desktop environment.

   The traditional file server architecture has many disadvantages especially with the advent of less expensive but more powerful computer hardware. The server directs the data while the workstation processes the directed data. Essentially this is a dumb server-smart workstation relationship. The server will send the entire file over the network even though the workstation only requires a few records in the file to satisfy the information request. In addition, an easy to use graphic user interface (GUI) added to this model simply adds to the network traffic, decreasing response time and limiting customer service.

   Unfortunately two defects limit a file server for multi-user applications.
   - The file server model does not support data concurrence (simultaneous access to a single data set by multiple user) that is required by multi-user applications.
   - If many workstations request and send many files in a LAN, the network can quickly become flooded with traffic, creating a block that degrades overall system performance.

WHAT IS CLEINT/SERVER?

Client/Server (C/S) refers to computing technologies in which the hardware and software components (i.e., clients and servers) are distributed across a network. The client/server software architecture is 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. This technology includes both the traditional database-oriented C/S technology, as well as more recent general distributed computing technologies.

Why Change to Client/Server Computing?

Client/Server is described as a 'costreduction' technology. This technology allows doing what one may be currently doing with computers much less expensively. These technologies include client/server computing, open systems, fourth generation languages, and relational databases. Cost reductions are usually quoted as the chief reasons for changing to client/Server. However, the list of reasons has grown to include improved control, increased data integrity and security, increased performance, and better connectivity. The key business issues dividing adoption are:

- Improving the Flow of Management Information
- Better Services to End-User Departments.
- Lowering IT costs
- The ability to manage IT costs better
- Direct access to required data
- High flexibility of information processing

Implementation examples of client/server technology:

- Online banking application
- Internal call centre application
- Applications for end-users that are stored in the server
- E-commerce online shopping page
- Intranet applications
- Financial, Inventory applications based on the client Server technology.
- Tele communication based on Internet technologies

Benefits of the Client/Server Technology:

Client/server systems offer the following benefits to the organisations

- People in the field of information systems can use client/server computing to make their jobs easier.
- Reduce the total cost of ownership.
- Increased productivity
- End user productivity
- Developer productivity
- Takes less people to maintain a client/server application than a mainframe
- The expenses of hardware and network in the client/server environment are less than that in the mainframe environment.
- Users are more productive today because they have easy access to data and because applications can be divided among many different users so efficiency is at its highest.
- Client/server applications make organisations more effective by allowing them to port applications simply and efficiently.
- Reduce the cost of computer the server stores data for the clients rather than clients needing large amounts of disk space. Therefore, the less expensive network computers can be used instead.
- Reduce the cost of purchasing, installing, and upgrading software programs and applications on each client's machine: delivery and maintenance would be from one central point, the server.
- The management control over the organization would be increased.
- Leads to new technology and the move to rapid application development such as object oriented technology.
- Long term cost benefits for development and support.

- Easy to add new hardware to support new systems such as document imaging and video teleconferencing which would not be feasible or cost efficient in a mainframe environment.
- Can implement multiple vendor software tools for each application.

Characteristics of Client/Server Technology:
There are ten characteristics that reflect the key features of a client/server system. These ten characteristics are as follows:

1. Client/server architecture consists of a client process and a server process that can be distinguished from each other.
2. The client portion and the server portions can operate on separate computer platforms.
3. Either the client platform or the server platform can be upgraded without having to upgrade the other platform.
4. The server is able to service multiple clients concurrently; in some client/server systems, clients can access multiple servers.
5. The client/server system includes some sort of networking capability.
6. A significant portion of the application logic resides at the client end.
7. Action is usually initiated at the client end, not the server end.
8. A user-friendly graphical user interface (GUI) generally resides at the client end.
9. A structured query language (SQL) capability is characteristic of the majority of client/server systems.
10. The database server should provide data protection and security.

APPROACHES TO CLIENT/SERVER
As mentioned earlier, 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" and a server is "any system or process that provides data, services, or access to other systems for clients, most often for multiple clients simultaneously". A simple definition of client/server computing is that server software accepts requests for data and presents the results to the user or, acting as a server, sends the results to the client that requested it. Client/server computing is based on the fact that it uses the programmable desktop computer to do most of its application processing. Even though the hardware in client/server computing is important, the focus needs to be on the technology that makes client/server computing possible which is the software.

Client/server computing allows applications to be broken down into many different jobs. "Each task can be run on a different platform, under a different operating system with a different network protocol. Each task can be developed and maintained separately accelerating application development".

Applications can be divided into six different tasks which include user interface, presentation logic, application logic, data requests and results acceptance, data integrity, and physical data management enabling many different IS professionals to work on the same application at the same time.

Client/server computing makes use of the divide and conquer logic. Client/server computing also allows users to access data easily resulting in all the data needed being close to the user. This helps users by allowing them to be more efficient and get applications done quicker than before when they did not have client/server computing. Client/server computing is making workers more productive. Both the client and the server in most of today's client/server networks perform processing.

Data storage, database management system, application software, operating system, user interface, and display devices are the major elements of this computing process. Data storage allows the retrieval of certain pieces of data, database management allows that data to be organized, and application software provides seamless integration of the two former elements at the user level. Operating systems control the resources of the computer system and allocate resources to meet the requests of the users. They control job scheduling, prioritize and allow access to support devices like

printers, and provide a communication channel between the client and the server. The user interface allows the end user to communicate with the application program. The interface could be a graphical user interface like Windows/Macintosh or character based as in DOS/Unix depending on the programming language. The last element in the model is the display device, which is the physical hardware that allows the operator to monitor and communicate with the user interface. This takes the form of a workstation or client.

COMPONENTS OF CLIENT SERVER ARCHITECTURE

Client: Clients, which are typically PCs, are the "users" of the services offered by the servers. There are basically three types of clients. Non-Graphical user Interface (GUI) clients require a minimum amount of human interaction; non-GUIs include ATMs, cell phones, fax machines, and robots. Second, GUI-Clients are human interaction models usually involving object/action models like the pull-down menus in Windows 3.x. Object-Oriented User Interface (OOUI) Clients take GUI-Clients even further with expanded visual formats, multiple workplaces, and object interaction rather than application interaction. Windows 95 is a common OOUI-Client.

Server: Servers await requests from the client and regulate access to shared resources. File servers make it possible to share files across a network by maintaining a shared library of documents, data, and images. Database servers allocate their processing power to execute Structured Query Language (SQL) requests from clients. Transaction servers execute a series of SQL commands, an online transaction-processing program (OLTP), as opposed to database servers, which respond to a single client command. Web servers allow clients and servers to communicate with a universal language called HTML.

Middleware: The network system implemented within the client/server technology is commonly called by the computer industry as middleware. Middleware is all the distributed software needed to allow clients and servers to interact. General middleware allows for communication, directory services, queuing, distributed file sharing, and printing. The middleware is typically composed of four layers, which are Service, Back-end Processing, Network Operating System, and Transport Stacks.

The Service layer carries coded instructions and data from software applications to the Back-end Processing layer for encapsulating network-routing instructions. Next, the Network Operating System adds additional instructions to ensure that the Transport layer transfers data packets to its designated receiver efficiently and correctly.

Fat-client or Fat-server: Fat-Client or Fat-server are popular terms in computer literature, describe the type of client/server systems in place. In a fat-client system, more of the processing takes place on the client, like with a file server or database server. Fat-servers place more emphasis on the server and try to minimize the processing done by clients. Examples of fat-servers are transaction, Group Ware, and web servers. It is also common to hear fat-clients referred to as ""2-Tier""systems and fat servers referred to as "3-Tier" systems.

Network: The network hardware is the cabling, the communication cords, and the device that link the server and the clients. The communication and data flow over the network is managed and maintained by network software.

CLIENT/SERVER SECURITY

Security procedures for client/server technology is not clearly defined or protected. As they utilise distributed techniques there is an increased risk of access to data and modification. To get secured client/server environment all access points should be known. As the application data may exist on the server or client, a number of access routes exist, which should be examined and checked.

To increase the security, systems personnel should ensure that the following control techniques are in place:

- Access to data and application is secured by disabling the floppy disk drive.
- Diskless workstation prevents unauthorised access.
- Unauthorized users may be prevented from overriding login scripts and access by securing automatic boot or startup batch files.
- Network monitoring can be done to know about the client so that it will be helpful for later investigation, if it is monitored properly. Various network-monitoring devices are used for this purpose. Since this is a detective control technique, the network administrator must continuously monitor the activities and maintain the devices, otherwise these tools become useless.
- Data encryption techniques are used to protect data from unauthorized access.
- Authentication systems can be provided to a client, so that they can enter into system, only by entering login name password.
- Smart cards can be used. It uses intelligent hand held devices and encryption techniques to decipher random codes provided by client-server based operating systems.
- Application controls may be used and users will be limited to access only those functions in the system that required to perform their duties.

CLIENT/SERVER RISKS AND ISSUES

The benefits from client/server are truly praiseworthy but there are also risks involved in the transition from mainframe (or PC) to client/server. We can classify these risks into four categories: technological, operational, economic, and political.

Technological Risks: The technological risk is quite simple-will the new system work? The short-term aspect of this question is-will it literally work? But more important is the 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 will it become obsolete. To resolve this issue the firm and the IT consultant/division should understand system standards and market trends and use them in their decision making processes while deciding what system to incorporate into their organization.

Operational Risks: These risks parallel the technological risks in both the short and long run. Respectively, they are: will we achieve the performance we need from the new technology and will the software that we choose be able to grow or adapt to the changing needs of the business. Once again sound planning and keeping an eye to the future are the only remedies for these risks.

Economic Risks: In the short run, firms are susceptible to hidden costs associated with the initial implementation of the new client/server system. Cost will rise in the short term since one needs to maintain the old system (mainframe) and the new client server architecture development. In the long run, the concern centres around the support costs of the new system.

Political Risks: Finally, political (people) risks involved in this transaction are addressed. Here, the short-term question is-will end users and management be satisfied? The answer to this is definitely not if the system is difficult to use or is filled with problems.

The long run question concerns costs. “Unless the mainframe is completely replaced within the larger organization, the total cost of transaction processing for the corporation as a whole goes up when one division creates its own independent system and moves off the mainframe. They may have reduced their local cost of transaction processing, but they have increased the cost of processing for divisions remaining on the mainframe, and this creates political problems”.

SERVER-CENTRIC MODEL

Server-Centric computing is a model, in which applications are deployed, managed, supported and executed 100% on a server. The client handles data entry and information display.

It uses a multi-user operating system and a method for distributing the presentation of an application's interface to a client device. With server-based computing, client devices, whether "fat" or "thin", have instant access to business-critical applications via the server-without application rewrites or download. This means improved efficiency when deploying business-critical applications. In addition, server-based computing work, within the current and future family of windows-based offerings to improve returns on computing investments-desktops, networks, applications and training. As the result, server-based computing is rapidly becoming the most reliable way to reduce the complexity and total costs associated with enterprise computing.

Traditionally used for centralizing business applications such as general ledger, payment order entry and point-of-sale applications, this recently expanded model now included web-based applications where users browse through data over the network. Almost any client device can be adapted for use with server-centric applications. Whether the user is using traditional terminals, GUI/Windows terminals, network computers, or personal computers, the overall solution's performance depends primarily on network bandwidth and the number of users connecting simultaneously. The more users accessing the server resources, the slower the response time.

This model enables enterprises to: bring heterogeneous computing environments providing access to Windows-based applications—regardless of client hardware, operating platform, network connection or LAN protocol. It offer enterprise-scale management tools to allow IT professionals to scale, deploy, manage and support applications from a single location, it also provide seamless desktop integration of the user's local and remote resources and applications with exceptional performance.

CHAPTER 7

SYSTEM DEVELOPMENT PROCESS

WHAT IS SYSTEM DEVELOPMENT PROCESS?

Computer information systems serve many different purposes, ranging from the processing of business transactions to providing information needed to decide recurring issues, assisting officials with difficult strategy formulation, and linking office information and corporate data.

In business, systems development refers to the process of examining business situation with the intent of improving it through better procedures and methods.

The process of system development starts when management or sometimes system development personnel realize that a particular business system needs improvement. Systems development can generally be thought of as having two major components.

-Systems analysis
-Systems design.

Systems analysis, is the process of gathering and interpreting facts, diagnosing problems and using the information to recommend improvements to the system. This is the job of system Analyst.

Systems design is the process of planning a new business system or one to replace or complement an existing system.

But before this planning can be done, one must thoroughly understand the old system and determine how computers can be used to make its operation more effective.

SYSTEM DEVELOPMENT LIFE CYCLE (SDLC):

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. The systems development life cycle consists of the following activities:

1. Preliminary investigation
2. Requirements analysis or systems analysis
3. Design of system
4. Development of software
5. Systems testing
6. Implementation and maintenance.

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 MIS department. This activity consists of three main sub functions.

-Request clarification
-Feasibility study and
-Request approval

Generally the requests which are submitted to the MIS department are not clearly stated. Hence, before any system investigations can be considered, the system request must be examined to determine precisely what the originator wants. Thereafter, the analyst tries to determine whether the system requested is feasible or not. Aspects of technical, economic and operational feasibility of the system are covered in the feasibility study. The third part of the investigation relates to approval of the request. Not all systems are desirable are feasible. Based on the observations of the analyst, the management decides which system should be taken up for development.

REQUIREMENT ANALYSIS OR SYSTEMS ANALYSIS

After studying the results of preliminary investigation, management decides to continue the development process; the needs of the users are studied. Analysts work closely with employees and managers of the organisation for determining information requirements of the users. Several fact-finding techniques and tools such as questionnaires, interviews, observing decision-maker behaviors and their office environment etc. are used for understanding 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. This step is also referred to as "systems analysis".

DESIGN OF THE SYSTEM

During system design, the user requirements that arose from analysing the user applications environment are incorporated into a new systems design. The analyst designs various reports/outputs, data entry procedures, inputs, files and database. He also selects file structures and data storage devices. These detailed design specifications are then passed on to the programming staff so that software development can begin.

ACQUISITION AND DEVELOPMENT OF SOFTWARE

After the system design details are resolved, such resource needs as specific type of hardware, software and services are determined. Subsequently, choices are made regarding which products to buy or lease from which vendors. Software developers may install or modify and install purchased software or they may write new, custom-designed programs. The choice depends on many factors such as time, cost and availability of programmers. The analyst works closely with the programmers if the software is to be developed in-house. During this phase, the analyst also works with users to develop worth while documentation for software, including various procedure manuals.

SYSTEMS TESTING

Before the information system can be used, it must be tested. Systems testing is done experimentally to ensure that the software does not fail i.e. it will run according to its specifications and in the way users expect. Special test data are input for processing, and results examined. If it is satisfactory, it is eventually tested with actual data from the current system.

IMPLEMENTATION AND MAINTANANCE

After the system is found to be fit it is implemented with actual data. Hardware is installed and users are then trained on the new system and eventually work on it is carried out independently. The results of the development efforts are reviewed to ensure that the new system satisfies user requirements. After implementation, the system is maintained, it is modified to adopt changing users and business needs so that the system can be useful to the organisation as long as possible.

The system development life cycle should be viewed as a continuous iterative process that recycles through each stage for many applications. Thus, even when a system is fully specified, designed, purchased and running, it is continually being enhanced or maintained. Enhancement and maintenance may require returning to one of the earlier stages of system development life cycle.

Achieving systems development objectives:

There are many reasons why organisations fail to achieve their systems development objectives. Although we cannot catalog all the reasons, we can summarize a few representative samples here:

- *Lack of senior management support for and involvement in information systems development:* Developers and users of information systems will watch senior management to determine which systems development projects are important and will act accordingly by shifting their efforts away from any project not receiving management attention.

- *Shifting user needs*: Users requirements for information technology are constantly changing. As these changes accelerate, there will be more requests for systems development and more development projects. When those changes occur during a development process, the development team may be faced with the challenge of developing systems whose very purposes have changed since the development process began.

- *Development of strategic systems:* Because strategic decision making is unstructured, the requirements, specifications, and objectives for such development projects are difficult to define; and determining "successful" development will be ambiguous.

- *New technologies:* When an organization tries to create a competitive advantage by applying advanced information technology, it generally finds that attaining systems development objectives is more difficult because personnel are not as familiar with the technology.

- *Lack of standard project management and systems development methodologies:* Some organizations do not formalise their project management and systems development methodologies, thereby making it very difficult to consistently complete projects on time or within budget.

- *Overworked or under-trained development staff:* Estimates of the backlog of systems development work facing development staffs range up to 4 years! In addition to being overworked, systems developers often lack sufficient education background. Furthermore, many companies do little to help their development personnel stay technically, currently in these organizations a training plan and training budget do not exist.

- *Resistance to change:* People have a natural tendency to resist change, and information systems development projects signal changes often radical in the workplace. Business process reengineering is often the catalyst for the systems development project. When personnel perceive that the project will result in personnel cutbacks, threatened personnel will dig on their heels, and the development project is doomed to failure. Personnel cutbacks often result when reengineering projects are really attempts at "downsizing" (or "rightsizing")

- *Lack of user participation:* Users must participate in the development effort to define their requirements, feel ownership for project success, and work to resolve development problems. User participation also helps reduce user resistance to change.

- *Inadequate testing and user training:* New systems must be tested before installation to determine that they will operate correctly. Users must be trained to effectively utilise the new system.

To overcome these and other problems, organizations must execute the systems development process efficiently and effectively.

APPROACHES TO SYSTEMS DEVELOPMENT

Several different systems development approaches are often used within an organisation. They are:

- Traditional Approach.
- Prototyping approach.
- End user Development approach.
- Top down approach.
- Bottom up approach.
- Systematic approach for development in small organisation.

Traditional Approach

In the traditional approach of the systems development, activities are performed in sequence. The following list shows tasks performed during each phase of the traditional approach.

Perception and expression of needs
Preliminary Investigation
Requirement Analysis
System design
System acquisition
System testing
System implementation & maintenance

Managers and users are most likely to interact with systems analysts, systems designers and application programmers when traditional approach is used. During the preliminary investigation and requirement analysis phases the user information needs are identified. Systems development activities are usually led by a systems analyst. During the later stages, they may turnover the project to system designers. When the traditional approach is applied, an activity is undertaken only when the prior step is fully completed. Managers and users consider and review the work performed by the MIS professionals during each stage of process before proceeding to the next stage. If the work is satisfactory, managers and users formally accept the work and allow the systems development team to proceed to the next step. It is important under traditional approach that managers and users should thoroughly review the work before granting this permission to start the next activity.

The traditional approach is applied to the development of larger computer based information systems such as the transaction processing systems.

Prototyping Approaches

The traditional approach sometimes may take years to analyse, design and implement a system. In order to avoid such delays organisations are increasingly using prototyping techniques. The goal of prototyping approach is to develop a small or pilot version called a prototype of part or all of a system. A prototype is a usable system or system component that is built quickly and at lesser cost, with an intention of being modifying or replacing it by a full-scale and fully operational system. As users work with the prototype, they make suggestions about the ways to improve. Those suggestions are then incorporated into another prototype, which is also used and evaluated and so on. Finally, when a prototype is developed that satisfies all user requirements, either it is refined and turned into the final system or it is scrapped. If it is scraped the knowledge gained from building the prototype is used to develop the real system.

Advantages of prototyping include:

-Improving the fact finding process
-Improving relations between analysts and users
-Encouraging the users to `own' the new system
-Reducing the cost of user training
-Identification of system problems
-Ensuring the quality of up coming system

Disadvantages of prototyping:

-Potential waste of time and money
-Potential cause of conflict between departments that all wants different things from the system.
-End-users mistakenly thinking that actual systems can be designed and developed at the same speed.

Top down approach:

The top down approach assumes a high degree of top management involvement in the planning process and focuses on organizational goals, objectives and strategies.

Using the top down approach, we begin by analyzing organizational objectives and goals and end by specifying application programs and modules that need to be developed to support those goals. The various stages in top down approach are as follows:

(a) Analyze the objectives and goals of the organization to determine where it is going and what management wants to accomplish.
(b) Identify the functions of the organization (for example, marketing, production, research and development) and explain how they support the entire organization.
(c) Based on the functions identified above, ascertain the major activities, decisions and functions of the managers at various levels of hierarchy. It should also be analyzed what decisions need to be made and when they should be made.
(d) With activities and decisions identified, we must now identify models that guide managerial decision processes and find out the information requirements for activities and decisions. An insight should be provided into what information is needed, when it is needed and what form is most useful.
(e) Prepare specific information processing programs in detail and modules within these programs. We may also identify files and data base for applications.

Bottom up approach:

The development of information system under this approach starts from the identification of life stream systems. Life stream systems are those which are essential for the day-to-day business activities. The examples of life stream systems include payroll, sales order, inventory control and purchasing etc. The development of information system, for each life stream system starts after identifying their basic transactions, information, file requirements and information processing programs.

After ascertaining the data/information requirements, files requirements and processing programs for each life stream system the information system for each is developed. The next step is towards the integration of data kept in different data files of each information system. The data is integrated only after thoroughly examining various applications, files and records.

The next step under bottom up approach may be the addition of decision models and various planning models for supporting the planning activities involved in management control. Further, these models are integrated to evolve model base. The models in the model base facilitate and support higher management activities. They are useful for analysing different factors, to understand difficult situations and to formulate alternative strategies and options to deal them.

A comparison of top down and bottom up approaches reveals the following points:

1. Top management takes the main initiative in formulating major objective strategies and policies, for developing MIS under top-down approach. In the bottom up approach it is the supervisory management who identifies the life stream systems for which MIS may be developed.
2. Middle and supervisory management levels has a little role in the development of system under top down approach.
3. The information system development under top down approach is more consistent with the systems approach and is also viewed as a total system, which is fully integrated. The information system developed under bottom up approach is developed through an orderly process of transition, building upon transaction processing sub-system. This system may not be integrated.

End User Development Approach

With the increasingly availability of low-cost technology, end user development is becoming popular in many organisations. In end-user development, it is the end user and not the computer professional who is responsible for systems development activities. Many different kinds of organisations allow end users to develop systems. The number and the nature of the steps followed in end user development is different with that of the formal approaches such as the traditional approach.

There are many risks involved in the end user approach, these include the following.

1. A decline in standards and controls: When an analyst is in-charge of developments, walk-through will be done and standards and policies will be enforced, these things are unlikely to be carried out to the same degree with end-user computing.
2. Inaccuracy of specification requirements: The end-user will not have the experience of an analyst in completing an accurate specification of system requirements.
3. Lack of adequate specifications: There would be reduction in the quality assurance and stability of the system.
4. Increase in unrelated and incompatible systems.
5. Difficulties in accessing could arise for users trying to access a central system, such as the corporate database, with a proliferation of different systems and applications.

Systematic Approach For Development In Small Organisations

In smaller organisations, fewer MIS professionals are employed and they may have such a variety of responsibilities that they have little time to develop new systems for users. Many smaller organisations developed good systems by using systematic approach even in the absence of MIS professionals. The systematic approach generally consists of the following steps:

Identify requirements
Locate, evaluate and secure suitable software
Locate, evaluate and select suitable hardware on which the above software can be run and implement the system

Stage I: THE PRELIMINARY INVESTIGATION

Systems development usually begins when a problem or opportunity is identified by managers and users. The purpose of the preliminary investigation is to evaluate the project request. It is neither a designed study, nor it includes the collection of details to completely describe the business system.

The analyst working on the preliminary investigation should accomplish the following objectives.

1. Clarify and understand the project request:
   What is presently being done?
   What is required and why?
   Is there an underlying reason different from the one the user has identified?
2. Determine the size of the project: The investigation towards this will gather the details useful in estimating the amount of time and number of people required to develop the project.
3. Determine the technical and operational feasibility of alternative approaches.
4. Assess costs and benefits of alternative approaches:
   What are the estimated costs for developing a particular system?
   Will the proposed system reduce operating costs?
   Will the proposed system provide better services to customers etc
5. Report findings to the management.

Conducting the Investigation

During preliminary investigation, the analyst collects the data through two primary methods.

1. *Reviewing internal documents:* The analysts conducting the investigation first try to learn about the organisation involved in, or affected by the project. Analysts can usually learn these details by examining organisation charts and studying written operating procedures.

2. *Conducting Interviews:* Written documents tell the analyst how the systems should operate, but they may not include enough details to allow a decision to be made about the merits of a systems proposal, nor do they present users views about current operations. To learn these details, analysts use interviews. Interviews allow analysts to know more about the nature of the project request and the reasons for submitting it.

Identifying Viable Options

After problems or opportunities are identified, the analyst must determine the scale of response needed to meet the user's requests for a new system as well as the approximate amount of time and money that will be required in the effort. The analysts then determine just how much management wants to spend on change.

Testing Project's Feasibility

After possible solution options are identified, project feasibility - the likelihood that these systems will be useful for the organisation is determined. Feasibility study refers to a process of evaluating alternative systems through costs/benefit analysis so that the most feasible and desirable system can be selected for development. The feasibility study of a system is undertaken from the following three angles:

1. Technical
2. Economical
3. Operational

Technical Feasibility

It is concerned with hardware and software. Essentially, the analyst ascertains whether the proposed system is feasible with existing or expected computer hardware and software technology. The technical issues usually raised during the feasibility stage of investigation include the following.

1. Does the necessary technology exist to do what is suggested? Can it be acquired?
2. Does the proposed equipment has the technical capacity to hold the data required to use the new system?
3. Will the proposed system provides adequate responses to inquires, regardless of the number or location of users?
4. Can the system be expanded if developed?
5. Are there technical guarantee of accuracy, reliability, case of access and data security?

A technically feasible system may not be economically feasible or may be so sophisticated that the firm's personnel cannot effectively operate it.

Economic Feasibility

It includes an evaluation of all the incremental costs and benefits expected if the proposed system is implemented. This is the most difficult aspect of the study. The financial and economic questions raised by analysts during the preliminary investigation are for the purpose of estimating the following.

1. The cost of conducting a full systems investigation.
2. The cost of hardware and software for the class of applications being considered.
3. The benefits in the form of reduced costs or fewer costly errors.
4. The cost if nothing is changed (i.e. the proposed system is not developed).

Operational Feasibility

It is concerned with ascertaining the views of workers, employees, customers and suppliers about the use of computer facility. The support or lack of support that the firm's employees are likely to give to the system is a critical aspect of feasibility. A system can be highly feasible in all respects except the operational and fails miserably because of human problems. Some of the questions, which help in testing the operational feasibility of a project, are stated below:

- Is there sufficient support for the system from management? From users? If the current system is well liked and used to the extent that persons will not be able to see reasons for a change, there may be resistance.
- Are current business methods acceptable to users? If they are not, users welcome a change that will bring about a more operational and useful system.
- Have the users been involved in planning and development of the project? Early involvement reduces the chances of resistance to the system.
- Will the proposed system cause harm? Will it produce poorer results in any respect or area? Will individual performance be poorer after implementation than before?

Estimating Costs and Benefits

After possible solution options are identified, the analyst should make a primary estimate of each solution's costs and benefits.

Costs: System costs can be subdivided into Development, Operational and Intangible costs.

Development costs for a computer based information system include:

1. Salaries of the system analysts and programmers who design and program the system.
2. Cost of converting and preparing data files and preparing systems manual and other supportive documents.
3. Cost of preparing new or expanded computer facilities.
4. Cost of testing the system, training employees and other startup costs.

Operating costs of a computer based system include:

1. Hardware software rental or depreciation charges.
2. Salaries of computer operators and other data processing personnel who will operate the new system.
3. Salaries of system analysts and computer programmers who perform the system maintenance function.
4. Cost of input data preparation and control.
5. Cost of maintaining proper physical facilities including power, light, heat, air conditioning building rental or other facilities.

Intangible costs of a computer based system include:

Intangible costs are the costs that can not be easily measurable. For example, the development of a new system may disturb the activities of an organisation and cause a loss of employee productivity or morale. Customer sales and goodwill may be lost by errors made during the installation of a new system. Such costs are difficult to measure in rupees but are directly related to the introduction and operation of information system.

Benefits: The benefits which result from developing new or improved system can be sub divided into Tangible and Intangible benefits.

Tangible benefits those that can be accurately measured and are directly related to the introduction of a new system, such as decrease in data processing costs.

Intangible benefits such as improved business image are harder to measure and define. Benefits that can results from the development of a computerized system are summarized below:

1. Increase in sales and profit.
2. Decrease in data processing costs.
3. Decrease in operating costs.
4. Decrease in required investment.
5. Increased operational ability and efficiency.

6. New or improved information availability.
7. Improved abilities in computation and analysis.
8. Improved customer service.
9. Improved employee morale.
10. Improved management decision making.
11. Improved competitive position.
12. Improved business image.

Reporting Results to Management

After the analyst articulates the problem and its scope, provides one or more solution alternatives and estimates the cost and benefits of each alternative, he reports these results to the management. From the analyst's report, management should determine what to do next. Not all projects submitted for evaluation and review are accepted. Primary investigation produces new information to suggest that improvement in management and supervision, and not the development of information systems are the actual solutions to the reported problems.

Stage II: REQUIREMENT ANALYSIS OR SYSTEMS ANALYSIS

This stage involves in determining user's needs, studying the present system of the organisation in depth, and determining the features that the new system should possess.

Requirements Analysis

If the management decides to continue developing the system after reading the analysts report, the requirement analysis phase of system development begins. Depends on the development approach the analysis will be carried out.

How thoroughly the present system is studied depends on the situation. To determine if the present system needs just a few adjustments instead of a complete change, the system should be studied in depth. However, if management is determined to replace the current system, it is better to spend time in determining exactly what management desires in new system.

While studying the present system the systems analyst must analyse how this system uses hardware, software and human resources to convert data into organisational information for end user needs. He should also analyse how these resources are used to accomplish the activity of input, processing, output, storage and control.

Fact finding techniques

Every system is built to meet some set of needs, to assess those needs, the analysts often interact extensively with the people, who will be benefited from the system. In order to determine what are their actual requirements system analysts uses various fact-finding techniques. Some of these fact-finding techniques used by the systems analysts are discussed below:

Documents:

Documents means manuals, input forms, output forms, diagrams of how the current system works, organisation charts showing hierarchy of users and manager responsibilities, job descriptions for the people who work with the current system etc. Documents are the very good source of information about user needs and the current system. They are easy to collect convey a lot of information and provide relatively objective data.

Questionnaires:

Questionnaires are very much useful when large amount of data details required from the users of existing system.

Interviews:
Users and managers may also be interviewed to extract information in depth. The data gathered through interviews often provide a systems developer with a complete picture of the problems and opportunities with the existing system.

Observation:
The analyst should visit the user site to watch how the work was taking place. The value of observation is very high, because what the systems analysts hears from users or reads from documents about the system is different from what he observes. In prototyping approach, observation plays a major role.

Analysis of the present system
Detailed investigation of the present system useful to understand the present system and its related problems.

The following are the areas studied while analysing the present system:

-Review of historical aspects.
-Analyse inputs.
-Review data files maintained.
-Review methods, procedures and data communications.
-Analyse outputs.
-Review internal controls.
-Model the existing physical system and logical system.

Review of historical aspects:
A brief history of the organisation is a logical starting point for an analysis of the present system. The historical facts are useful to identify the following.

-Major turning points and milestones that have influenced
-Historical perspective through review of annual reports
-Growth of management levels
-Development of various functional areas and departments
-Operations that have been successful or unsuccessful with computers.

Analyse Inputs:
A detailed analysis of present inputs is important to analyst because he will be able to determine how these inputs fit into the framework of the present system. The system analyst must study the following while analysing the inputs. He can also understand that how the outputs of one system can be used as input for another parts of the system.

-Where the data are initially captured?
-Nature of each form, What is contained in it?
-Who prepared it?
-From where the form is initiated?
-Where it is completed?
-Distribution of the form

Review data files maintained:
The analyst should investigate the data files maintained by each department, noting their number and size, where they are located, who uses them. The system analyst should also review all on-line and off-line files which are maintained in the organisation as it is useful to understand about the data that are not contained in any outputs. Based on the review, he can determine the data requirements of the proposed system.

Review methods, procedures and data communications:
Methods and procedures transform input data into useful output. A method is defined as 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 the methods by which each job is accomplished the equipment utilized and the actual location of the operations. This review is useful for the following:

-To eliminate unnecessary tasks
-To perceive improvement opportunities
-To understand the data communications used
-Devices and methods used in data communications

Analyse outputs:
The outputs should be studied carefully by the system analyst in order to determine.
-How they meet the organisation's needs?
-What information is needed?
-Why the information needed?
-Who needs the information?
-When they needs the information?
-Where it is needed?

By studying these, the analyst can attempt to eliminate all such reports which are not relevant to the new system.

Review internal controls:
A detailed investigation of the present system is not complete until internal control is reviewed. An analysis of present system of internal controls may indicate weaknesses that should be removed in the new system.

Model the existing physical system and logical system:
As the logic of inputs, methods, procedures, data files, data communications, reports, internal controls and other important items are received and analysed in a top down manner, the process must be properly documented.

The logical flow of the present information system may be depicted with the help of system flow charts. The physical flow of the existing system may be shown by employing data flow diagrams.

The flow charting and data flow diagramming of present information system not only organizes the facts, but also helps in disclose gaps and duplication in the data gathered.

Undertake overall analysis of present system
Based upon the aforesaid investigation of the present information system, the final phase of the detailed investigation includes the analysis of:

The present work volume
The current personnel requirements
The present benefits and costs

Systems Analysis of Proposed System
After each functional area of the present system has been carefully analysed, the proposed system specifications must be clearly defined. These specifications are determined from the desired objectives set out at the first stage of the study. The required systems specifications which should be in conformity with the projects objectives are as follows:

- Outputs produced with great emphasis on timely managerial reports that utilise the 'management by exception' principle.
- Database maintained with great accent on online processing capabilities.
- Input data prepared directly from original source documents for processing by the computer system.
- Methods and procedures that show the relationship of inputs and outputs to the database, utilizing data communications where deemed appropriate.
- Work volumes and timings carefully considered for present and future periods including peak periods.

The starting point for compiling these specifications is output. After outputs have been determined, it is possible to infer what inputs, database, methods, procedures and data communications must be employed. The output-to-input process is recommended since the outputs are directly related to the objectives of the organisation. After completing the various steps mentioned above, the information gathered is documented in the explanatory survey report, which is authorised and signed by the team of system analysts and approved by the user group. This report is then presented to the steering committee.

SYSTEMS DEVELOPMENT TOOLS

Many tools and techniques have been developed to improve current information systems and develop new systems. Such tools help end users and systems analysts to:

- Conceptualise, clarify, document and communicate the activities and resources involved in the organisation and its information systems.
- Analyse present business operations, management decision making and information processing activities of the organisation.
- Propose and design new or improved information systems to solve business problems

Many systems development tools take the form of diagrams and other graphic representations. The major tools used or system development can be grouped into four categories based on the systems features each document has:

-Components and flows of a system
-User interface
-Data attributes and relationships
-Detailed system process.

Each of these categories are explained below

System Components and Flows

These tools help the system analyst to document the data flow among the major resources and activities of an information system. The tools in this category are

1. System Flow chart
2. Data Flow diagram
3. System components matrix

User Interface

Designing the interface between end users and the computer system is a major consideration of a system analyst while designing the new system.

1. Layout forms and screens
2. Dialogue flow diagram

Data Attributes and relationships

The data resources in information system are defined, catalogued and designed by the following category of tools.

1. Data dictionary
2. Entity-relationship diagrams
3. File layout forms

Detailed system process

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

1. Structure charts
2. Decision tables
3. Decision trees

Some of these tools are described below:

System flowchart:

It is a graphic diagramming tool that documents and communicates the flow of data, media and information processing procedures taking place in an information system. System flowcharts typically emphasize the media and hardware used and the processes that take place within an information system. Thus, system flowcharts represent a graphic model of the physical information system that exists or is proposed.

Data Flow Diagrams:

Data flow diagrams show how data flow within organisation. The data flow diagram does not depict any physical components rather it shows the logical descriptions of system elements. The term, structured analysis is commonly used to refer to the preparation of data flow diagram.

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. Layout forms and screens are used to design source documents, input/output and storage, records, files and output displays and reports.

System Components Matrix:

The system components matrix can be used as an information system frame work for both systems analysis and system design. It views the information system as a matrix of components that high lights how the 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.

It highlight the basic information processing activities needed in the organisation, resources used and products produced by this system.

CASE Tools:

The data flow diagram and system flowcharts that users review are commonly generated by systems developers using the on-screen drawing modules found in CASE (Computer Aided Software Engineering) software packages. CASE refers to the automation of any thing that humans do to develop systems. In earlier days these tools enabled system analysts and programmers to create flowcharts and data flow diagrams on mini computer or microcomputers. Today, CASE products can support virtually all phases of traditional system development process.

CASE Tools include menu generator, screen generator, report generator and code generator.

Menu Generator:
Menu generators outline the functions or components of system. When linked to other menus, they illustrate how users can branch to various screens and subscreens used for data entry or inquiry.

Screen Generators:
Screen generators are used for design reports on screen, to format or "point" the desired layouts and content of a screen without having to enter complex formatting information.

Report Generators:
Report generators are similar to screen generators in that formats are generated in the same fashion. In addition they can indicate totals, paging, print edits, sequencing and control breaks in creating samples of the desired systems report.

Code Generators:
Code generators allow the analyst to generate the modular units of source code from the high level specifications provided by the system analyst, demonstrate the system, revise specifications and demonstrate the system again.

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, a data dictionary is a computer file containing the data about the data. It contains the following information about the data in the files:

1. Codes describing the data items length, data type and range.
2. The identity of the source document used to create the data item.
3. The names of the computer files that store the data item.
4. The names of the computer programs that modify the data item.
5. The identity of the computer programs or individuals permitted to access the data item for the purpose of file maintenance, upkeep, or inquiry.
6. The identity of the computer programs or individuals not permitted to access the data item.

Uses:
a. It helps as a documentation tool to programmers and system analysts, who performs operations on the database or computer programs that access these database.
b. It is also useful for file security by restricting the file access.
c. An auditors can make use of a data dictionary for establishing audit trail on data items there by on input sources and the computer programs that use these sources.
d. It can serve as an important aid when investigating or documenting internal control procedures.

CHAPTER 8

SYSTEMS DESIGN

The system design is one of the core components in the systems development process of an Information system. The requirement analysis stage primarily defines the ways things are, the system design stage defines the way things should be.

Stage III: **SYSTEMS DESIGN**

After the completion of requirements analysis for a system, systems design activity takes place for the alternative which is selected by management. The system design phase usually consists of following three activities.

1. Reviewing the system's 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
3. Reporting results to management.

The system's design must conform to the purpose, scale and general concepts of the system that management approved during the requirements analysis phase. Therefore, users and system analysts must review each of these matters again before starting the design because they establish both the direction and the constraints that system developers must follow during rest of the activities.

System design involves first logical design and then physical construction of a system. When analysts formulate a logical design, they write the detailed specifications for the new system, they describe its features, the outputs, input files, databases and procedures, all in a manner that meets systems requirements. The statement of these features is termed as the design specifications of the system.

Logical Design

The logical design of an information system is like an engineering blueprint, it shows major features of the system and how they are related to one another. The reports and outputs of the system are like the engineer's design components.

Physical Construction

Physical construction, the activity following logical design, produces program software, files and a working system. Design specifications instruct programmers about what the system should do. The programmers write the programs that accept input from users, process data, produce the reports, and store data in the files.

Developing a model for a new system

When designing a system, the systems analysts and systems development team determines how the system components will be realised at logical and physical levels in each of the following areas:

Output
Processing
Storage
Procedures and
Personnel

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.

One of the most important features of an information system for users is the output it produces. Without quality output, the entire system may appear to be so unnecessary that users will avoid using it, possibly causing it to fail.

Designing computer output should proceed in an organised, well thought out manner. The right output must be developed while ensuring that each output element is designed so that users will find the system easy to use effectively.

Output Objectives:

The output from an information system should accomplish one or more of the following objectives:

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

Good systems output design can not be developed independent of the uses of the output. In other words, more attractive output or even output that uses innovative computer technology can not be classified as good unless it meets the needs of the organisation and its users.

Important factors in output design:

There are six important factors which should be considered by the system analyst while designing user outputs, these are:

Content
Form
Volume
Timeliness
Media
Format

Content:

Contents refers to the actual pieces of data included among the outputs provided to users. For example, the contents of a weekly report to a sales manager might consist of sales person's name, sales calls made by each sales person during the week, and the amount of each product sold by each sales person to each major client category. The contents should be only the information required by the user.

Form:

Form refers to the way that content is presented to users. Content can be presented in various forms

Quantitative
Non-quantitative
Graphics
Audio.

Various department managers often prefer both summary and detailed information to be presented in relative terms or in chart form such as pie chart, line chart or bar chart rather than information in absolute terms. Some times, converting absolute values to relative values such as percentages often help managers to comprehend the data easily and make better decisions.

Output Volume:

The amount of data output required at any one time is known as output volume. It is better to use high speed printer or a rapid-retrieval display unit which are fast and frequently used output devices in case the volume is heavy.

Timeliness:

Timeliness refer to when users need outputs. Some outputs are required on a regular, periodic basis, perhaps daily, weekly, monthly, at the end of a quarter or annually. Other types of outputs are generated on request.

Media:
Input-output media refers to the physical device used for input, storage or output. A variety of output media are available in the market these days which include paper, video display, microfilm, magnetic tape, disk and voice output. The system designer can select medium, which is best suited to the user requirements.

Format:
The manner in which data are physically arranged is referred to as format. This arrangement is called output format when referring to data output on a printed report or on a display screen.

How to present information?
In this section we will discuss guidelines for presenting tabular and graphic information.

TABULAR FORMAT:
In general, end users are most accustomed to receiving information in a tabular form. Accountants and those who regularly review financial data rely exclusively on tabular information. Common examples of tabular reports are inventory control, accounts payable, general ledger, sales analysis and production scheduling reports. In general, the tabular format should be used when details dominate and few narrative comments or explanations are needed.

Certain information in a tabular format is more important and should be more visible than other information. In general the following list should be included in tabular reports.

Exceptions to normal exceptions.
Major categories or groups of activities.
Summaries of major categories or activities.
Unique identification information.
Time dependent entities.

The system analyst must design tabular output to show these elements distinctively.

GRAPHIC FORMAT:
Graphic systems are available across a wide range of prices and capabilities and from personal computers to mainframes. Due to the availability of low cost but powerful computer software that uses data from existing databases and produces high quality charts and diagrams, graphics outputs are becoming very popular. Graphics are used for several reasons. They are used to improve the effectiveness of output reporting for the targeted recipients, to manage information volume and to suit personal preferences.

Standards in designing graphics:
In designing graphical output, the systems analyst must determine 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 outputs. Graphic output also contains text, the design of which is an important aspect. Each graphic report, whether printed or displayed, should include a title and the date of preparation. For a series, page numbers should also be included. Labels can increase the accuracy with which people read data which is in graph form.

Graphical output can be enormously useful to decision makers if they are trained how to interpret it and when to use it. Without the training, it is doubtful whether graphs mean much to the users.

Designing printed output
A printed output layout is the arrangement of items on the output medium. The layout is a blue print that will guide the construction of programs later in the development process. To begin the design of a layout, it is necessary to determine what items will be included in the report. The requirements

analysis phase provides this information, and the data dictionary contains necessary descriptive information such as data item type and length etc.

There are certain guidelines which should be followed while preparing the layout form. Some of these guidelines are summarised below:

1. Reports and documents should be designed to read from left to right and top to bottom.
2. The most important items should be easiest to find.
3. Each printed report should include the heading or title of the report, page number, date of preparation and column headings. The heading or title should be numbered so that the user has an easy point of reference when discussing output with others. The date of report preparation should be included, this helps users to estimate the value of the output.
4. Each data item must have a heading, which should be short and descriptive.
5. Control breaks should be used in the report to help readability. They should be separated from the rest of the data with additional lines. Attention should be drawn to control breaks summaries and other important information.
6. Sufficient margin should be left on the right and left as well as top and bottom of an output report. This enables the user to focus his attention on the material centered on the page and makes reading easier.

Designing visual display output

Many of the principles of good design discussed for printed output are also applied to output that is shown on video display terminal. It should be noted that a visual display terminal offers less space to work with compared to most printed outputs. Moreover, the system analyst is also required to give instructions to the user on how to use the display unit.

Layout of display screen

Each display page is commonly called a screen or panel. Designing a layout begins with verifying the characteristics of the display screen. These include:

- Physical dimensions of the screen.
- Number of rows and columns of data that can be displayed.
- Degree of resolution.
- Number of colours available.
- Methods of highlighting.

Screen design begins with the recognition that the screen is composed of different areas. In designing output screens, we need areas for.

- Headings and titles.
- Content of the display.
- Messages and instructions.
- Explanations for the information in the report.

Usually the headings and titles are positioned at the top portion of the screen, messages and instructions at the bottom, and explanations if needed, on the right hand side. However, it is mainly a matter of preference of the concerned system analysts.

Designing of windows

In computer output, windows are sub-divisions of the display screen that make it possible to present different sets of output simultaneously users can run several programs at the same time, displaying the output from each in an individual window. Or a single program can present more than one output simultaneously.

The use of windows should be considered when the applications are required to be improved by the following abilities:

- Display different data or report sets simultaneously.
- Switch between several programs, alternatively displaying the output from each.
- Move information from one window to the other.
- Allow individual user to reposition the information on a display screen to suit their unique needs.

These situations are common to one or more of the following examples:
Order enquiries:
When reviewing a customer order, an assistant will find it helpful if one window can display the firm's product catalogue another the details of the specific order in question, and the third the specific data from the customer invoice.

Accounts payable verification:
In accounts payable systems, customer description details (name, address) are shown in one window and current month purchase, payment and adjustment transactions in another. This example demonstrates the simultaneous display for identification and transaction details.

DESIGNING SYSTEMS INPUTS

Input design consists of

- Developing specifications and procedures for data preparation.
- Developing steps which are necessary to put transactions data into a usable form for processing.
- Data entry

Among the input issues to consider for design of input specifications are

Content
Timeliness
Media
Format
Volume

Content:
The analyst is required to consider the types of data that are needed to be gathered to generate the desired user outputs. This can be quite complicated because new systems often mean new information and new information often requires new sources of data. Sometimes, the data needed for a new system are not available within the organisation. Hence, the system designer has to prepare new documents for collecting such information.

Timeliness:
In data processing, it is very important that data is inputted to computer in time because outputs cannot be produced until certain inputs are available. In transaction processing the people needing output are not the same who input most of the data. Hence, timeliness of input becomes more relevant for such systems.

Media:
Another important input consideration includes the choice of input media and subsequently the devices on which to enter the data. Various user input alternatives available in the market include display workstations, magnetic tapes, magnetic disks, key-boards, optical character recognition, pen-based computers and voice input, etc.,

Format:
After the data contents and media requirements are determined, input formats are considered. While specifying the record formats, for instance, the type and length of each data field as well as any other special characters must be defined.

Input Volume:
Input volume refers to the amount of data that has to be entered in the computer system at any one time. In some decision-support systems and many real-time systems input volume is low. In batch-oriented transaction processing systems, input volume could be heavy which involves thousands of records that are handled by a centralized data entry department using key-to-tape or key-to-disk systems.

Capturing Data for Input
The quality of system inputs determines the quality of system output. It is vital that input forms and screens be designed with this critical relationship in mind. Well designed input forms and visual display terminal screens should meet the objectives of effectiveness, accuracy, ease of use, consistency, simplicity and attractiveness. All these objectives can be attained if the analyst keeps in mind the basic design principles, knowledge of what is needed as input for the system, and an understanding how users respond to different elements of forms and screens.

FORM DESIGN
Forms are pre-printed papers that require people to fill in responses in standardised way. Forms often serve as source documents for the data entry personnel.

GUIDELINES FOR FORM DESIGN
The following guidelines for form design should be observed in order to design useful forms.

Making Forms easy to Fill.
Meeting the intended purpose.
Ensuring accurate completion.
Keeping forms attractive.

Making Forms easy to Fill
To reduce errors, speed-up completion and facilitate entry of data, it is essential that forms should be easy to fill out. This can be achieved by considering the following factors.

(a) Form flow: Designing form with proper flow can minimise time and effort expended by employees in a form completion. Forms should flow from left to right and top to bottom. Illogical flow takes extra time and can be frustrating for the user.

(b) Divide forms in logical sections: The second technique that makes it easy for people to fill out form correctly is logical grouping of information. A form consists of seven main sections namely (i)headings, (ii)Identification and Access, (iii) Instructions, (iv) Body, (v)Signature and Verifications, (vi) Totals and, (vii) Comments.

The heading section includes the name and address of the business originating the form. The identification and access section includes codes that may be used to fill the report and gain access to it at a later date. Instructions indicates how to fill the form. Body section includes the details to be completed. The signature and verification section includes authorised persons signature and verification. Totals include summary data of the form. The comments part shows comments on the form contents.

(c) Captioning: Clear captioning is yet another technique that can make easy work of filling up the form. Captions tell the persons completing the forms what to put on a blank line space or box.

Meeting the intended purpose
Forms are created to serve one or more purposes in the recording, processing, storing and retrieving of information for various business. Sometimes it is desirable to provide different information to different departments or users while still sharing same basic information. This is where specialty

forms are useful. The analyst can use his imagination to design such forms which can provide the information required by different departments while avoiding duplication of information.

Ensuring accurate completion

Error rates typically associated with collecting data can drop sharply when forms are designed to assure accurate completion. Design is important in making people to do the right thing with the form. Various controls can be included in the form design. For example, the form design can provide an internal double check with column totals and row totals, summing to the same number. If the row and column totals do not sum to the same number, the user filling out the form knows that there is a problem and can correct it immediately.

Keeping form attractive

Forms should look uncluttered, organized and logical even after they are filled in. To be attractive, forms should present information in the expected order. Convention dictates asking for name, address, city, state and pin code in this order. Using different fonts for type with in the same form can help in making it attractive for the user. Separate categories and sub-categories with thick and thin lines can also encourage user to use the form.

CODING METHODS

Information systems projects are designed with space, time and cost saving in mind. Hence, coding methods in which conditions, words or relationships are expressed by a code are developed to reduce input, control errors and to speed up entire process.

A code is a brief number, title or symbol used instead of lengthy or ambiguous description. Descriptions are particularly unsuited for computerized applications. They are usually too long and would require much higher computer time for processing than the codes. Therefore, when an event occurs, the details of the event are summarised by the code, with code, fewer details are necessary to input but it results in no loss of information.

Some of the desired characteristics of a good coding Scheme are:

- Individuality
- Space
- Convenience
- Expandability
- Suggestiveness
- Permanence

Individuality:

The code must identify each object in a set uniquely and with absolute precision. To use one code number for several objects in a set would obviously cause a great deal of confusion. Furthermore, the code should be universally used over the entire organization.

Space:

As far as possible a code number must be much more brief than description.

Convenience:

The formats of code numbers should facilitate their use by people. This implies that the code number should be short and simple and consist of digits and or upper case alphabets. It is better to avoid the use of such special symbols as hyphens, slashes, dot, etc.,

Expandability:

As far as possible future growth in the number of objects in a set should be provided for. Therefore, whilst introducing the scheme, longer number of digits/number than necessary at present may be adopted as the code length.

Suggestiveness:
The logic of the coding scheme should be readily understandable. Also, the letter or number should be suggestive of the item characteristics. But this should not be carried too far in lengthening the code since it would defeat the purpose of briefing.

Permanence:
Changing circumstances should not invalidate the scheme or invalidation in the future should be kept to minimal.

Coding Schemes:
Various commonly used coding schemes.

Classification Codes.
Function Codes.
Significant-digit subset Code.
Mnemonic Code.
Hierarchical classification.

Classification Codes:
Classification Codes separate entities, such as events, people, or objects into distinct groups called classes. The Classification Code is used to distinguish one class from another. The Code is recorded on the source document by the user. In an online system, it can be keyed directly into the system through a terminal. The user classifies the event into one of the several possible Categories and records the Code. Classification Codes vastly simplify the input process because only a single digit Code is required. The need for writing lengthy descriptions is eliminated and hence the process is made simpler.

Function Codes:
Function Codes state the activities or work to be performed without spelling out all of the details in narrative statement. For example, appending or updating a record in a transaction processing system would require only the identification key of the record and the Function Code.

Significant-digit subset codes:
A well conceived coding scheme, using significant digit subset codes, can provide a wealth of information to users and management. One way to accomplish this is to assign numbers in sequence, starting with the first and going through to the last and a prefix can be added to the identification numbers to further describe the type of item.

Codes can be divided into subsets or subcodes, characters that are part of the identification number and that have special meaning. The subcode give the user additional information about the item. In the inventory example, the most important information is the class of product, the item within that class, and the supplier.
Using digits in an identification number to convey additional information does not add to length of the data or, to processing time. However, the extra information that sub codes provide more information to the management.

Mnemonic Codes:
These are suitable where the codes have to be remembered by people eg. BL may stand for bolts. Universities frequently use mnemonics to code information: MBA for master of Business Administration or CS for Computer science etc.,

Hierarchical classification:
This scheme groups items based on one code and sub classification is made on further classes and items.

DESIGNING EFFICIENT DATA ENTRY

Assuring the quality of data input to the information system is critical to assure quality output. The quality of data entered can be improved through attainment of the three major data entry objects these are:

Effective and efficient data capture.
Effective coding.
Appropriate data-entry methods.

As has been discussed earlier,

- A well designed form to serve as a source document is the first step towards effective data capture.
- A second way to speed up data entry is through effective use of coding, which puts data in short sequences.
- Finally, effective data entry can be achieved by giving attention to the input devices being used.

Data can be input through many different methods, each with varying speed and reliability. Efficiency improvement on key-to-tape has been realized through the invention of key-to-disk and key-to-floppy diskette systems. Reading of data through use of special machines (MICR, OCR etc.,), which eliminates the process of transcription of source data into machine-readable form and also requires less employee skills.

Along with appropriate coding, data capture and input devices, accurate data entry can be enhanced through the use of input validation. Input transactions should be checked to assure that the transaction requested is acceptable, authorized and correct. Input data can be validated through inclusion in the software of several types of tests that check for missing data, length of data item, range and reasonableness of data and invalid values of data.

DATA STORAGE:

Storing data is often an important decision in the design of an information system. There are two approaches for storing data. The first approach is to store data in individual files, one file for each application. The second approach is to develop a data base that can be shared by many users for a variety of applications as need arises.

The conventional file approach may at times be a more efficient approach since the file can be application oriented. On the other hand, the data base approach may be more appropriate because the same data need to be entered, stored and updated once. Examples of conventional files include master files, table files, transaction files, work files, and report files. They can have a sequential organization, random or direct organization, indexed organization, or indexed-sequential organization. These are the most effective ways of organizing and storing data in transaction systems where each transaction is processed to update a record in the master file. However, when the purpose of the information system is to support management decision-making and same data is used in multiple applications, the analyst may find that these methods of file organization are inadequate and he may have to adopt data base approach.

Although systems analysts do not design database, a separate database management staff oversees the design and development of the database. However, the analyst must work with data base administrators to determine how data will be stored and what methods will be used for their retrieval and conversion to the format the program requires. Analysts are responsible for identifying and satisfying user requirements by drawing on the data stored in the database, and, where appropriate, by developing independent master and transaction files.

SYSTEM MANUAL:

The basic output of the system design is a description of the task to be performed, complete with layout and flowcharts. This is called the job specifications manual or system manual. It contains:

1. General description of the existing system.
2. Flow of the existing system.
3. Outputs of the existing system-the documents produced by existing system are listed and briefly described, including distribution of copies.
4. General description of the new system-its purposes and functions and major differences from the existing system are stated together with a brief justification for the change.
5. Flow of the new system-this shows the flow of the system from and to the computer operation and the flow within the computer department.
6. Output Layouts
7. Output distribution- The distribution of the new output document is indicated and the number of copies, routing and purpose in each department shown. The output distribution is summarized to show what each department will receive as a part of the proposed system.
8. Input layouts-the inputs to the new system are described and complete layouts of the input documents and input disks or tapes provided.
9. Input responsibility- the source of each input document is indicated as also the user department responsible for each item on the input documents.
10. Macro-logic-the overall logic of the internal flows will be briefly described by the systems analyst, wherever useful.
11. Files to be maintained-the specifications will contain a listing of the tape, disk or other permanent record files to be maintained, and the items of information to be included in each file. There must be complete layouts for intermediate or work file; these may be prepared later by the programmer.
12. List of programs - a list of the programs to be written shall be a part of the systems specifications.
13. Timing estimates-a summary of approximate computer timing is provided by the systems analyst.
14. Controls - this shall include type of controls, and the method in which it will be operated
15. The audit trail for all financial information. It indicates the method with which errors and defalcation will be prevented or eliminated.
16. Glossary of terms used.

REPORTING TO MANAGEMENT

After the system design is finished, users have indicated their satisfaction with the design, and the system's benefits and costs are revised to reflect any major changes, the system development team reports the results of these activities to the management. The report should include.

1. Description of the application and users source that led to the system.
2. A summary of the results of the requirement analysis.
3. Design recommendation.
4. Any change in the costs and benefits of the new system.
5. A plan for the remaining system development activities.

If the management is satisfied with the work the systems developer will proceed to the next phase of the systems development process.

CHAPTER 9
SYSTEMS ACQUISITION SOFTWARE DEVELOPMENT AND TESTING

STAGE IV: **SYSTEMS ACQUISITION AND SOFTWARE DEVELOPMENT**

After a system is designed, either partially or fully, the next phase of the systems development starts which relates to the acquisition of hardware, software and services. In this section, we will explore how this process takes place.

ACQUIRING SYSTEMS COMPONENTS FROM 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 systems being developed. These physical items are identified after the logical design of the system model is finished. After the management gives its consent to go a head with the project, the acquisition process starts.

Acquiring the appropriate hardware and software is critical for the success of the whole project. The organization can discover new hardware and software developments in various ways. The system development team often prepares a list of specific needs. Management also decides whether the hardware is to be purchased, leased from a third party or to be rented. The system development team then approaches various vendors who, in turn, respond with specific systems and prices. After vendor alternatives are known, one or more methods may be used by the team to select specific resources.

PROCURING COMPUTER HARDWARE:

The following points may be considered while selecting a computer system:

1. All computer systems offered in the market today have good hardware, competent software and roughly similar facilities. Due to the rapid development of computer technology, the more recent the computer, the better its performance is and the lower its cost. Therefore, as far as possible, the latest possible technology should be acquired.
2. Commercial data processing consists mainly of reading-in-data, printing out data and storing and retrieving information from magnetic media. Thus, computer performance for commercial work is mainly determined by the speeds and capabilities of input/output and storage peripherals. Scientific, engineering and operations problems require good computational facilities. Thus, the efficiency of a computer in handling such problems will depend on the main storage available and the instruction execution speed. A comparison along these lines can be made quickly and quite effectively for selecting hardware.
3. Experts maintain that since hardware speed and facilities are uniformly good, today the selection of computer should be made on software considerations. While all manufacturers supply general software packages for linear programming. PERT, etc., and packages for such commercial applications as inventory control and production planning, a few manufacturers also offer packages specially designed for a particular industry such as packages for airline reservations and packages for applications in banking and insurance. Sometimes the superiority of software may not be strong enough to influence a computer acquisition decision.
4. Modern computers are marketed as series of compatible machines with increasingly powerful central processors and interchangeable peripherals. This is very useful when, after a few years, work expands to fit in the existing computer storage and a bigger machine is required. A more capable machine of the same series will allow the existing programs to be carried over so that the large investment in programming may be preserved. In case of breakdown, compatibility allows a wider range of machines to be used as back-up. Thus, the choice of a computer really becomes a choice of a model within a series, based on a long-range plan of expansion.
5. The selection of a computer does not end within the choice of a manufacturer and a model. It continues to the selection of a configuration and a plan for its gradual expansion. This can be as important as the choice of manufacturer and a properly considered model can save a great deal of money. Outside assistance in computer selection can be had from computer manufacturers, independent consultants specializing in computers, or management consulting firms.

SOFTWARE ACQUISITION: Make or buy:

Once user outputs and input designs are finalised, the nature of the applications software requirements must be assessed by the systems analyst. This determination helps the systems development team to decide what type of application software products are needed and consequently, the degree of processing that the system needs to handle. This helps the system developers in deciding about the nature of the systems software and computer hardware that will be most suitable for generating the desired outputs.

The analysis of output and input needs suggests numerous processing requirements for application software. From these requirements, the systems analyst is able to determine the basic functions and capabilities that the software must posses. At this stage, the system developers must determine whether the application software should be created in-house or acquired from a vendor. This decision is often called the make-or-buy decision. In the past several years, pre-written application software or application software packages have become increasingly popular for many business functions, including accounting (for example, payroll and personnel accounting) general ledger, manufacturing, financial planning and numerous other applications. Many of these packages consist of several programs and a complete set of documentation tools. Vendors providing these software packages even impart training about how to use the software to its full potential.

Advantages of Application Packages: The four most compelling advantages of using pre-written application packages are summarized below:

1. Rapid implementation: Application packages are readily available to implement after they are purchased. In contrast, software developed in-house may take months or even years until it is ready for implementation.
2. Low risk: Since the application package is available in the finished form, the organization knows what it is going to get for the price it has paid. With in-house developed software, the long development time breeds uncertainly with regard to both the quality of the final product and its final cost.
3. Quality: The firms engaged in application package development are typically specialist in their products' area. Generally, they have lot of experience in their specialised application field and hence can provide better software. In contrast, in-house programmers often have to work over a wide range of application areas; they may not be possessing expertise for undertaking proposed software development.
4. Cost: Software vendors can leverage the cost of developing a product by selling the product to several other firms, thereby realizing a lower cost from each application user. Thus, an application package generally costs less than an in-house developed package. Hence, application packages, sometimes, turn out to be cheaper compared to in-house developed software.

Sources of Packaged Software:

Thousands of programs are available in the market today for purchase. Computer manufacturers, large and small software houses and computer retail stores are some of the sources from where these packages can be purchased. Another source of packaged software is user groups or association of users of a particular computer system. User groups often recognise the need for a specific program, which may be developed by one member organisation and made available to other members. For example, utility programs and extension of existing operation systems are typically developed by a member organisation and distributed through the user group.

Assessment of Packaged software:

The assessment of packaged software considered for purchases is quite difficult. The following features of a package may be ascertained before purchasing the same:

1. Can the program provide the needed reports?

2. Does the program have adequate capacity in terms of the number of transactions it can process, the number and length of fields per record it can process, the total file size permitted and so on?
3. How many processing runs on the computer are required to complete each data processing job? Some programs will perform several tasks each time they are executed. Others may perform only one task per run and hence a program may have to be executed several times, requiring more operator time and computer processing to complete the job.
4. How long does the program take to process? The efficiency of program processing varies considerably among the programs that perform the same task. Some may require much more time compared to other programs.

Current users of a software package are a valuable source of information about its performance. They usually describe both the unanticipated problems and the unexpected benefits of a particular program. Reputable vendors normally provide the list of various users of the package and hence it is desirable to contact any of these users before purchasing software. An alternative way of evaluating a package is to actually process data with it on the organization's own computer. This process is called software bench mark test and consists of using the organizations transactions to access the processing speed, user friendliness of the program and the operation of special features such as report-writing capabilities. Preparation of a software bench-mark test is considered to be a difficult task since only experienced persons in actual operation over a long period of time can provide a full test of the advantages and limitations of the software package.

STEPS INVOLVED IN SELECTION OF A COMPUTER SYSTEM

The selection of an appropriate computer demands a high level of expertise and many organisations use a consultant either to provide guidance to their personnel or to manage this activity.

The steps involved in selection of a computer system are:

1. Prepare the design specifications.
2. Prepare and distribute an RFP (Request for proposal) to selected computer vendors.
3. On the basis of an analysis of proposals, eliminate vendors whose proposals are inferior.
4. Have vendors present their proposals.
5. Conduct further analysis of the proposals.
6. Contact present users of the proposed systems.
7. Conduct equipment benchmark tests.
8. Select the equipment.

During feasibility study, the EDP manager will list down various requirements of the organisation based on which design specifications of the computer will be laid down. These mandatory specifications would then constitute an over-riding criterion of selection. If a vendor fails to meet them, the manager would simply screen out that vendor without any further consideration. These specification would establish a desired configuration that might include for example, the required minimum main memory size, the required characteristics of secondary memory, and general types and capacities of input and output equipment needed etc usually, design specifications should be developed without reference to any specific models of equipment or to a particular vendor's product line.

Generally, a RFP (request for proposal) is prepared by the organisation and given to vendors, asking the vendors to prepare a bid and submit it to the organisation. The RFP contains all details that are necessary for a vendor to prepare a fully detailed proposal. After responses to RFP have been received, they are evaluated by the organisation. Usually each vendor, whose bid is competitive in terms of price and meeting the requirements of the RFP is asked to make a presentation to explain the bid and the products proposal. During the presentation, the organisation's representatives enquire about all aspects of the vendor's recommendations and bid.

The after presentation equipment analysis is carried out in even greater details, and it involves the proposals of only those vendors who remain in competition which may be only one or two. At this point, the organisation should be satisfied that the systems still being considered can solve its problems in a cost effective manner. If this is not the case, the drastic steps of rewriting the design specifications and of submitting RFPs to other vendors must be considered.

VALIDATION OF VENDORS' PROPOSALS

This process consists of evaluating and ranking the proposals submitted by vendors and is quite difficult, expensive and time consuming, but in any case it has to be gone through. The following factors have to be considered towards rigorous evaluation.

1. **The Performance Capability of Each Proposed System in Relation to its Costs:** It is imperative that vendor system be capable of processing the organisation's data within the time frames desired by management. Otherwise, delays in providing needed outputs will occur once the computer system is operational. There are many measures of performance, including speed, response time, number of users supported, and system testing. One way to examine the operating efficiency of a particular system is to use a benchmark test.
2. **The Costs and Benefits of Each Proposed System:** The accountants on the design team will analyze the costs of every vendor's proposed system in relation to the system's anticipated performance benefits—i.e., they will perform a cost-benefit analysis for each proposed system. In this effort, the accountants should also investigate the differences between purchasing and leasing each vendor'' system.
3. **The Maintainability of Each Proposed System:** Maintainability refers to the case with which a proposed computer system can be modified. For example, this flexibility enables a firm to alter a portion of a payroll system to reflect new federal tax laws. Because the costs of maintaining a large information system are typically five times as much as the costs of initially acquiring or developing a system, the evaluators should place considerable emphasis on this dimension.
4. **The compatibility of each proposed system with existing systems:** Compatibility refers to the ability to implement and interface the new system with existing computer resources and software. In some instances, this comes down to hardware issues. For example, it may not be possible to run specific software modules of the new system on some of the company's older local area network servers, which will consequently have to be upgraded. But compatibility issues can also involve the operating system, existing application software, or procedural concerns as well-for example, the requirement that employees learn a whole new set of procedures for inputting data.
5. **Vendor support:** vendor support includes such things as (1) training classes that familiarize employees with the operating characteristics of the new system, (2) help in implementing and testing the new system, (3) assistance in maintaining the new system through a maintenance contract, and (4) backup systems for temporarily processing company data if required. The availability of "business-hours-only" versus "round-the-clock" support is another consideration. Most vendors charge extra for enhanced services.

Methods of validating the proposal:

The following are some of the validation methods.

1. *Checklists:* It is the most simple and rather a subjective method for validation and evaluation. The various criteria are put in checklist in the form of suitable questions against which the responses of the various vendors are validated. Obviously, then, the vendor who has most cleverly responds is likely to get the award. Below given an example of software checklist and a support service checklist.

   a. Example of software validation checklist:
   1. What is the package designed to do?
   2. How developed is the software package?

3. How is the package organised?
4. Is the package operable?
5. Can the package operate on our hardware configuration?
6. Can the program provide the needed reports?
7. Does the program have adequate capacity in terms of the number of transactions it can process, the number and length of fields per record it can process, the total file size permitted and so on?
8. How many processing runs on the computer are required to complete each data processing job? Some programs will perform several tasks each time they are executed. Other may perform only one task per run and hence a program may have to be executed several times, requiring more operator time and computer processing to complete the job.
9. How long does the program take to process? The efficiency of program processing varies considerably among the programs that perform the same task. Some may require much more time compared to other programs.
10. Will the package require modifications?
11. Can the package be modified if necessary?
12. Who will modify the package?
13. What are the overall costs?
14. Is comprehensive documentation available?
15. Who will maintain the package?
16. What are the package constraints?
17. Where is the package currently utilised?
18. What is the primary language?
19. What input/output techniques are utilised?
20. What are the required input/output formats?
21. How must input can be organised?
22. What controls are included?
23. What kind of user training is provided?

b. Example of support service checklists

1. Performance: what has been the vendor's past performance in terms of his promises?
2. System development: are system analysis and programming consultants available what are their qualities and cost?
3. Maintenance: is equipment maintenance provided? What is the quality and cost?
4. Conversion: what systems development, programming and hardware installation service will they provide during the conversion period?
5. Training: is the necessary training of personnel provided? What is its quality and cost?
6. Back-up: Are several similar computer facilities available for emergency backup purposes?
7. Proximity: Does the vendor have a local office? Are sales, systems development, programming, and hardware maintenance services provided from the office?
8. Hardware: Do they have a wide selection of compatible hardware?
9. Software: Do they have a wide variety of useful systems software application programs?

Similar checklists may be developed for hardware compatibility etc. This method however is generally applied only to minor proposals.

2. *Point-Scoring Analysis:* Another approach for evaluating those packaged software is a point-scoring analysis such as the one illustrated below.
   When performing a point-scoring analysis, the evaluation committee first assigns potential points to each of the evaluation criteria based on its relative importance. In the table, for example, the committee feels that "adequate controls" is more important than whether "other users are satisfied with the software" they assign relevant scores.

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 determines the winner. Thus, in the following table, the evaluation indicates the vendor B packages has the highest total and the committee should therefore acquire this vendor's system.

Software evaluation criteria	Possible points	Vendor A	Vendor B	Vendor C
Does the software meet all mandatory specifications?	10	7	9	6
Will program modifications, if any, be minimal to meet company needs?	10	8	9	7
Does the software contain adequate controls?	10	9	9	8
Is the performance (speed, accuracy, reliability) adequate?	10	7	9	6
Are other users satisfied with the software?	8	6	7	5
Is the software user-friendly?	10	7	8	6
Can the software be demonstrated and test-driven?	9	8	8	7
Does the software have an adequate warranty?	8	6	7	5
Is the software flexible and easily maintained?	8	5	7	5
Is online inquiry of files and records possible?	10	8	9	7
Will the vendor keep the software up to date?	10	8	8	7
Total	123	94	106	85

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 has been frequently and usefully employed by several buyers in the past. For those criteria, however, where published reports are not available, resort would have to be made to other methods of validation. This method is particularly useful where the buying staff has inadequate knowledge of computer facts.

Bench marking 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 workload. They include software considerations and can be current applications programs or new programs that have been designed to represent planned processing needs i.e., benchmarking problems are oriented towards testing whether a computer offered by the vendor meets the requirements of the job on hand of the buyer. Obviously, benchmarking problems can be applied only if job mix has been clearly specified. The benchmarking problems, would then comprise long jobs, short jobs, tape jobs, disk jobs, mathematical problems, input and output loads etc, in proportion typical of the job mix. If the job is truly represented by the selected benchmarking problems, then this approach can provide a realistic and tangible basis for comparing all vendor's proposals.

Bench marking problems, however, suffer from a couple of disadvantages. It takes considerable time and effort to select problems representative of the job mix which itself must be precisely defined. It also requires the existence of operational hardware, software and services of systems. Nevertheless, this approach is very popular because it can test the functioning of vendor's proposal.

Test problems:

Test problems disregard the actual job mix and are devised to test that are true capabilities of the hardware, software or system. For example, test problems may be developed to evaluate the time required to translate the source code (program in an assembly or a high level language) into the object code (machine language), response time for two or more jobs in multi-program, length of time required to execute an instruction etc. The results, achieved by the machine can be compared and price performance judgement can be made. However the various capabilities to be tested would have to be assigned relative weightage.

SOFTWARE DEVELOPMENT

If the organization decides that all the software for the application under consideration is to be developed in-house, then the organization must put considerable efforts on program development. The development of application software also undergo a life cycle similar to the one used to develop the entire system. An in-house creation of programs commonly involves the following six stages called the program development life cycle.

1. *Program analysis:* In this stage, the programmer ascertains for a particular application (e.g., up-dating of the stock file), the outputs required (i.e., the up-dated stock file, listing of the replenishment orders), the inputs available (i.e., up-dating the physical balance, computing stock value for various items, determination of placement of the replenishment order etc). The programmer then determines whether the proposed application can be or should be programmed at all.

2. *Program design:* In this stage, the programmer develops the general organization of the program as it relates to the main functions to be performed. Out of several other tools available to him, input, output and file layouts form design tools and flowcharts are quite useful at this stage. These layouts and flowcharts etc. are provided to the programmer by the systems analyst.

3. *Program Coding:* The logic of the program outlined in the flowcharts is converted into program statements or instructions at this stage. For each language, there are specific rules concerning format and syntax. Syntax means vocabulary, punctuation and grammatical rules available in the language manuals, which the programmer has to follow strictly. There are special sheets for writing the program instructions in each language. The format of these sheet facilitates writing error-free programs.

   The programmers broadly pursue three objectives while writing programs: simplicity, efficient utilization of storage and least processing time. It is highly desirable that the programs are simple to understand since a program written by one programmer is very difficult for the other to understand. Further, the programs, upon implementation, may require frequent modification to suit the changing systems environment. There is a program maintenance group employed on a permanent basis for modifying the programs and this group is different from the one who wrote the programs initially. It is, therefore, emphasized that programs should be written as simple as possible to start with. There is usually a trade off possible between the other two objectives: efficient utilization of storage and least processing time.

4. *Debug the program:* The process of debugging a program refers to correcting programming language syntax and diagnostic errors so that the program “compiles cleanly”. A clean compile means that the program successfully converted from the source code written by the programmer into machine language instructions. Once, the programmer achieves a clean compile, the program is ready for structured walk through discussed below.

   Debugging can be a tedious task. It consists of four steps: inputting the source program to the compiler, letting the compiler find errors in the program, correcting lines of code that are in error, and resubmitting the corrected source program as input to the compiler. Usually, this process must be repeated half a dozen or more times using a batch compiler. The length of time required to debug a program can be shortened considerably by the use of an interactive compiler which checks the source program and displays any errors on a CRT. The programmer corrects the indicated errors and initiates the interactive compiler as often as necessary until all errors are corrected. The interactive compiler allows the programmer to debug a program in a few hours, as opposed to a few days using a batch compiler.

   Use structured walkthroughs: After a program has been compiled and scrutinized for obvious errors, there is need for a structured walkthrough is a mental execution of the program by the

programming team. In order to perform walkthroughs, the programming team must examine the source text after which the team meets and collectively performs a mental execution of the program. A list of errors is made as each logical path is followed. The interfaces with modules either calling or called by the module being examined are carefully checked as well. At the end of the walkthrough, the list of errors is given to the author of the program. Using this approach, most errors are caught before any testing occurs. Also, the team members who review the text become familiar with parts of the system other than their own. This helps to establish a common base of understanding of all components of the system.

Test the program: A careful and thorough testing of each program is imperative to the successful installation of any system. Approximately 30 to 50 percent of the resources required for program development should be allocated to program testing. The programmer should plan the testing to be performed, including testing all possible exceptions. The test plan should require the execution of all standard processing logic. The program test plan should be discussed with the project manager and/or system users. A log of test results and all conditions successfully tested should be kept maintained to avoid repeated testing.

Review the program code for adherence to standards: One of the preliminary steps of the systems implementation phase is to set standards for program coding. It is necessary to review each program to ensure that standards are being met (various programming standards are discussed later) ideally someone who is not directly connected to the implementation team should review it, so that the quality of the system and adherence to standards are evaluated objectively without concern for project schedule and budget.

5. Program documentation: The writing of narrative procedures and instructions for people who will use software is done throughout the program life cycle. Managers and users should carefully review documentation in order to ensure that the software and system behave as the documentation indicates. If they do not, documentation should be revised. User documentation should also be reviewed for understandability i.e., the documentation should be prepared in such a way that the user can clearly understand the instructions and it should not be presented in a computer jargon which only sophisticated MIS professional can comprehend.

6. Program maintenance: The requirements of business data processing applications are subject to continual change. This calls for modification of the various programs. There are, usually separate categories of programmers called maintenance programmers who are entrusted with this task.

PROGRAM DESIGN TOOLS

We will now briefly discuss some of the several program design tools which are now-a days available.

Program flow chart:

Program flow chart is among the most common program design tools that managers and users encounter when reviewing the design work of the system development project. Program flow charts were discussed in detail in Intermediate study material. These flowcharts depict the logical steps through which a computer program must proceed when solving a problem. At one time, program flow charts were considered the premier program design tool. Although they are still widely used, sometimes it is difficult for programmers to translate a program flow chart directly into a structured code.

A program flow chart depicts the logical processing steps followed by a program quite well, however, unlike some of the other program design tools, they often do not provide a broad view of how the program is organized.

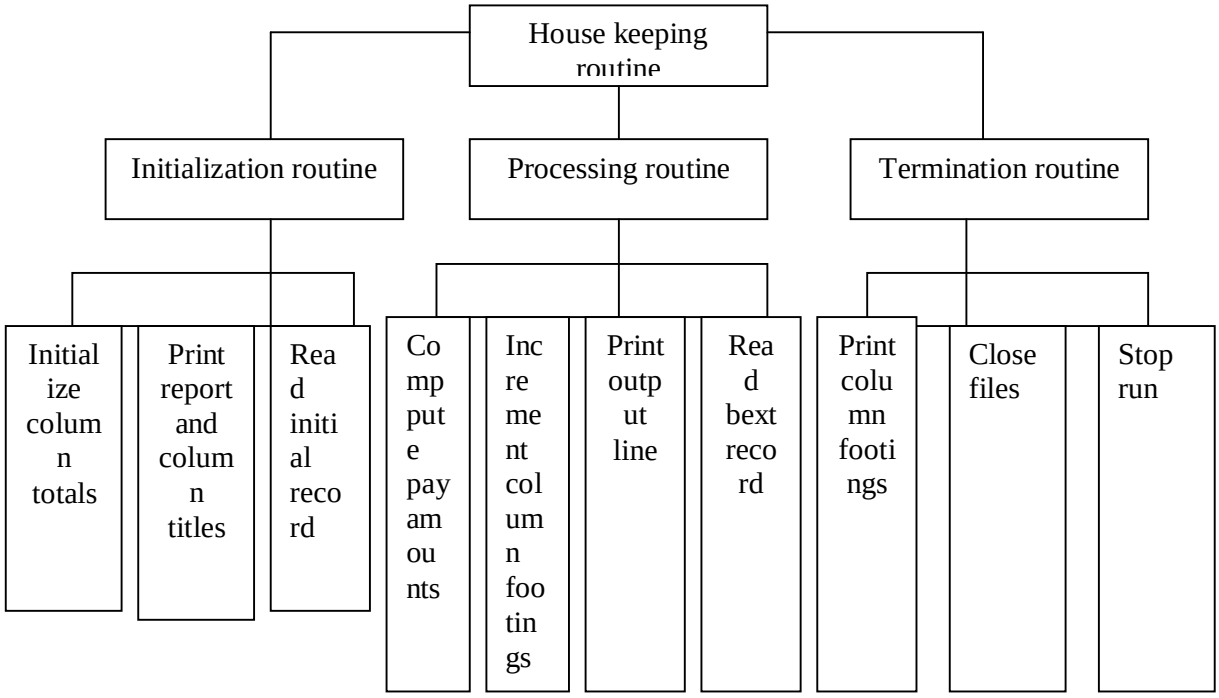
Pseudo code:

When reviewing the work done by a program designer, users may also need to review narrative descriptions of program logic. Pseudo code, like program flow charts, also represents program logic. However, instead of using graphical symbols and flow lines, pseudo code presents program logic in English-like statements. Pseudo code is generally preferred by programmers over flowcharts because it represents program code more closely.

Pseudo code is used in a variety of ways. For example many fourth-generation languages use pseudo code-like statements. Often, these statements can be translated directly into 3 GL program code, such as COBOL etc. besides using pseudo code to design program code in a 3GL, it can be embedded into a completed 3GL program as non executable 'comment' statements (i.e. those statements which are not translated by the compiler into object code) that serve as a documentation to indicate what the program is doing. Pseudo code is particularly useful when designing transaction processing and information-retrieval programs. Program flowchart, in contrast, are most useful for abstract types of user problems, that is, problems involving many mathematical or scientific formulae.

Structure chart:

Another type of program design tool that a user may review is the program structure chart. Structure charts, which look similar to corporate organization charts, are useful for organizing problems. The structure chart organizes each of the program tasks into well-defined modules. The higher-level-modules represent control portions of the program; the lowest level modules do the actual task of the program. Unlike either flow charts or pseudo code, the structure chart does not give any detail of the actual program logic and the order in which various tasks are executed. Instead they show how all the logical functions of the program fit together as a whole.



4GL Tools:

The various tools described above were developed as manually applied methods for designing programs or systems. The main drawback of manually applied tools is that they take a lot of time to prepare. Also, when a program flow chart is prepared or a structure chart is drawn, the programmer is not sure if it is internally consistent. Fourth-generation languages provide a way out to remove these obstacles by automating many of these manual tasks by using 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.

Object oriented programming and design tools:

These tools provide a means of enhancing programmer productivity and of reducing the application backlogs common in many organizations. Object oriented software design results in a model that describe object, classes and their relationships to one another. The object oriented design is often taken from a data flow diagram (DFD). In fact, every input and output screen, every process and data store found in a fully decomposed DFD may be a candidate for an object in an object-oriented design. There is a wide variety of object oriented development tool kits available in the market. For example, Microsoft's Application provides an integrated object oriented program development system that includes (1) tools for creating and manipulating objects, (2) a visual programming environment for constructing object and application interfaces, and (3) a shell that supports either object oriented programming or traditional structured program.

By adopting 4GL and object-oriented programming tools, the organizations can decrease their application development time substantially.

STAGE V: **SYSTEM TESTING**

System-level testing must be conducted prior to installation of an information system. It involves:

(a) preparation of realistic test data in accordance with the system test plan:
(b) processing the test data using the new equipment,
(c) through checking of the results of all system tests, and
(d) reviewing the results with future users, operators and support personnel.

System level testing is an excellent time for training employees in the operation of the IS as well as maintaining it. Typically, it requires 25 to 35 per cent of the total implementation effort.

One of the most effective ways to perform 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 data files and output results.

For an interactive information system project, the process of running dual operations for both new and old system is more difficult than it is for a batch-processing system. One procedure for testing the 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 on the old system. The outputs are checked for compatibility, and appropriate corrections are made to the on-line computer programs. Once this segment of the new system has proved satisfactory, the entire terminal network can be placed into operation for this on work. Additional sections of the system can be added by testing in this manner until all programs are operational.

During parallel operations, the mistakes detected are often not those of the new system, but of the old. These differences should be reconciled as far as it is feasible economically. Those responsible for comparing the two systems should clearly establish that the remaining deficiencies are cause by the old system. A poor checking job at this point can result in complaints later from customers, top management, salespersons, and others.

CHAPTER 10

SYSTEMS IMPLEMENTATION AND MAINTENANCE

The process of ensuring that the information system is operational and then allowing users to take over its operation for use and evaluation is called systems implementation. Implementation includes all those activities that take place to convert from the old system to the new. The new system may be totally new, replacing an existing manual or automatic system or it may be major modification in an existing system. In either case, proper implementation is essential to provide a reliable system to meet organizational requirements. In this chapter we will discuss four aspects of implementation:

- Equipment installation
- Training personnel
- Conversion procedures and
- Post-implementation evaluation.

EQUIPMENT INSTALLATION

The hardware required to support the new system is selected prior to the implementation phase. The necessary hardware should be ordered in time to allow for installation and testing of equipment during the implementation phase. An installation checklist should be developed at this time with operating advice from the vendor and system development team. In those installations adequate time should be scheduled to allow completion of the following activities:

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

   In case of a mini computer, or a mainframe, the Project Manager should prepare a rough layout, make cost estimates and get budget approved from the management. Layout planning must be done well in advance in order to permit acquisition for long lead time items like air-conditioning equipment, etc. the following factors should be taken into consideration for space planning:
   - space occupied by the equipment
   - space occupied by the people; and
   - movement of equipment and people.

2. *Equipment installation:* The equipment must be physically installed by the manufacturer, connected-to the power source and wired to communication lines if required.

3. *Equipment check out:* The equipment must be turned on for testing under normal operating conditions. Not only the routine diagnostic test should be run by the vendor, but also the implementation team should devise and run extensive tests of its own to ensure that equipment are in proper working condition.

TRAINING PERSONNEL

A system can succeed or fail depending on the way it is operated and used. Therefore, the quality of training received by the personnel involved with the system in various capacities helps or hinders the successful implementation of information system. Thus, training is becoming a major component of systems implementation. When a new system is acquired which often involves new hardware and software, both users and computer professional generally need some type of training. Often this is imparted through classes, which are organized by vendor and through hands-on learning techniques.

Training systems operators: Many systems depend on the computer-center personnel, who are responsible for keeping the equipment running as well as for providing the necessary support services. Their training must ensure that

- They are able to handle all possible operations, both routine and extra-ordinary and it must also involve the data entry personnel.
- If the system call for the installation of new equipment, such as a new computer system, special terminals or data-entry equipment, the operators training should include such fundamentals as how to turn the equipment on and use it, and knowledge of what constitute normal operation and use.
- The operators should also be instructed in what common malfunctioning may occur, how to recognize them, and what steps to take when they arise.
- As part of their training, operators should be given both a trouble shooting list that identifies possible problems and remedies for them, as well as the names and telephone numbers of individuals to contact when unexpected or unusual problem arise.

User training:
User training may involve equipment use, particularly in the case where a micro-computer is in use and the individual involved is both operator and user. In these cases, users must be instructed first how to operate the equipment.

- User training must instruct individuals involved in trouble shooting of the system, determining whether the problem is caused by the equipment or software or by something they have done in using the system.
- Most user training deals with the operation of the system itself.
- Users should be trained on data handling activities such as editing data, formulating enquiries (finding specific records or getting responses to question) and deleting records of data.
- Some training time should be devoted to such system maintenance activities as to prepare disks, load paper into printers, or change ribbons on printers.

CONVERSION OR CHANGE PROCEDURES
Conversion or changeover is the process of changing from the old system to the new system. There are many conversion strategies available to the analyst who has to take into account several organizational variables in deciding which conversion strategy to use. It may be noted that adequate planning and scheduling of conversion as well as adequate security are more important for a successful changeover.

Conversion strategies: There are five strategies for converting from the old system to the new one:

1. *Direct changeover:*
   Conversion by direct changeover means that on a specified date, the old system is dropped and the new system is put into use. Direct changeover can only be successful if extensive testing is done beforehand. An advantage of the direct changeover is that users have no possibility of using the old system other than the new system.

   Direct changeover is considered a risky approach to conversion, and disadvantages are numerous. For instance
   - long delays might ensue if error occur, since there is no other way to accomplish processing.
   - Additionally, users may dislike being forced into using an unfamiliar system without recourse.
   - Finally, there is no adequate way to compare new results with old.

2. *Parallel conversion:*
   This refers to running the old system and the new system at the same time, in parallel. This is the most frequently used conversion approach, but its popularity may be decline because it works best when a computerized system replaces a manual one. Both systems are run simultaneously for a specified period of time and the reliability of results is examined. When the same results are gained over time, the new system is put into use and the old one is stopped.

The advantage of running both systems in parallel includes the possibility of checking new data against old data in order to catch any errors in processing in the new system. Parallel processing also offers a feeling of security to users, who are not forced to make a sudden change to the new system.

There are many disadvantages to parallel conversion. These include
-the cost of running two systems at the same time, and
-the burden on employees of virtually doubling their workload during conversion
-unless the system being replaced is a manual one, it is difficult to make comparisons between output -of the new system and the old one
-it is understandable that employees who are faced with a choice between two system will continue using the old one because of their familiarity with it.

3. *Gradual conversion:*
Gradual conversion attempts to combine the best features of the earlier two plans, without incurring the risks. In this plan, the volume of transactions is gradually increased as the system is phased in. The advantages include allowing users to get involved with the system gradually and the possibility of detecting and recovering from the errors without a lot of downtime.

Disadvantages of gradual conversion include taking too long to get the new system in place and its inappropriateness for conversion of small uncomplicated systems.

4. *Modular prototype conversion:*
This approach to conversion uses the building of modular, operational prototypes to change from old systems to new in a gradual manner. As each module is modified and accepted, it is put into use. One advantage is that each module is thoroughly tested before being used. Another advantage is that users are familiar with each module as it becomes operational.

The fact that many times prototypes is not feasible which automatically rules out this approach for many conversions. Another disadvantage is that special attention must be paid to interfaces so that the modules being built actually work as a system.

5. *Distributed conversion:*
This refers to a situation in which many installations of the same system are considered, such as in banking or in franchises such as restaurants or clothing stores. One entire conversion is done (with any of the four approaches considered already) at one site. When that conversion is successfully completed, other conversions are done for other sites.

An advantage of distributed conversion is that problems can be detected (and contained) rather than force them, in succession, on all sites. A disadvantage is that even when one conversion is successful, each site will have its own peculiarities to work through and these must be handled.

Activities involved in conversion:
Conversion includes all those activities, which must be completed to successfully convert from the previous system to the new information system. Fundamentally these activities can be classified as follows:

1. Procedure conversion
2. File conversion
3. System conversion;
4. Scheduling personnel and equipment;
5. Alternative plans in case of equipment failure.

1. *Procedure conversion:*
Operating procedures should be completely documented for the new system. This applies to both computer-operations and functional area operations. Before any conversion activity can start,

operating procedures must be clearly spelled out for personnel in the functional areas undergoing changes. Information on input, data files, methods, procedures, output, and internal control must be presented in clear, concise and understandable terms for the average reader. Written operating procedures must be supplemented by oral communication during the training sessions on the system change.

2. *File conversion:*
   Because large files of information must be converted from one medium to another, this phase should be started long before, after programming and testing are completed. The cost and related problems of file conversion are significant whether they involve on-line files (common database) or off-line files. Present manual files are likely to be inaccurate and incomplete where deviations from the accepted format are common. These files suffer from the shortcomings because of maintenance by inexperienced-and, at times, indifferent-personnel. Computer generated files tend to be more accurate and consistent. If the existing system is operating on a computer but of different configuration, the formats of the present computer files are generally unacceptable for the new system.

   Besides the need to provide a compatible format, there are several other reasons for file conversion. The files may require character translation that is acceptable to the character set of the new computer system. Data from floppy disks, magnetic tapes, and comparable media will have to be placed on magnetic disk and/or mass storage files in order to construct an on-line common database. Also, the rearrangement of certain data fields for more efficient programming may be desired.

   In order for the conversion to be as accurate as possible, file conversion programs must be thoroughly tested. Adequate control, such as record counts and control totals, should be required as output of the conversion program. The existing computer files should be kept for a period of time until sufficient files are accumulated for back-up. This is necessary in case the files must be reconstructed from scratch after a "bug" is discovered later in the conversion routine.

3. *System conversion:* After on-line and off-line files have been converted and the reliability of the new system has been confirmed for a functional area, daily processing can be shifted from the existing information system to the new one. A cut-off point 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. System development team members should be present to assist and to answer any questions that might develop, consideration should be given to operating the old system for some more time to permit checking and balancing the total results of both systems. All differences must be reconciled. If necessary, appropriate changes are made to the new system and its computer programs. 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 information system for the first time is a difficult task for the system manager. As users become more familiar with the new system, however, the job becomes more routine.

   Schedules should be set up by the system manager in conjunction with departmental managers of operational units serviced by the equipment. The master schedule provides 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 reruns, programs testing, special non-recurring reports and other necessary runs.

   Just as the equipment must be scheduled for its maximum utilization, so must be personnel who operate the equipment. It is also imperative that personnel who enter input data and handle output data be included in the data processing schedule. Otherwise, data will not be available when the

equipment needs it for processing. It is essential that each person follow the methods and procedures forth by the MIS section; non-compliance with established norms will have an adverse effect on the entire system.

5. *Alternative plans in case of equipment failure:* Alternative processing plans must be implemented in case of equipment failure. Who or what caused the failure is not as important in case of equipment failure as the fact that the system is down. Priorities must be given to those jobs critical to an organization, such as billing, payroll, and inventory. Critical jobs can be performed manually until the equipment is set right.

   Documentation of alternative plans in the responsibility of the computer section and should be fully covered by the organization's systems and procedures manual. It should state explicitly what the critical jobs are, how they are to be handled in case of equipment failure, where compatible equipment is located, who will be responsible for each area during downtime and what dead-lines must be met during the emergency. A written manual of procedures concerning what steps must be undertaken will help expedite the unfavorable situation. Otherwise, panic will result in the least efficient methods when time is of the essence.

EVALUATION OF THE NEW SYSTEM

The final step of the systems implementation is evaluation. Evaluation provides the feedback necessary to assess the value of information and the performance of personnel and technology included in the newly designed system. This feedback serves two functions:

1. It provides information as to what adjustments to the information system may be necessary.
2. It provides information as to what adjustments should be made in approaching future information systems development projects.

There are two basic dimensions of information systems that should be evaluated. The first dimension is concerned with whether the newly developed system is operating properly. The other dimension is concerned with whether the user is satisfied with the information system with regard to the reports supplied by it.

Development Evaluation:

Evaluation of the development process is primarily concerned with whether the system was developed on schedule and with in budget. This is a rather straightforward evaluation. However, it requires schedules and budgets to be established in advance and that records of actual performance and cost be maintained. However, it may be noted that very few information systems have been developed on schedule and within budget. In fact, many information systems are developed without clearly defined schedules or budgets. Due to the uncertainty and mystique associated with system development, they are not subjected to traditional management control procedures.

Operation evaluation:

The evaluation of the information system's operation pertains to whether the hardware, software and personnel are capable to perform their duties and they do actually perform them so. Operation evaluation answers such questions:

1. Are all transactions processed on time?
2. Are all values computed accurately?
3. Is the system easy to work with and understand?
4. Is terminal response time within acceptable limits?
5. Are reports processed on time?
6. Is there adequate storage capacity for data?

Operation evaluation is relatively straightforward if evaluation criteria are established in advance. For example, if the systems analyst lays down the criterion that a system which is capable of

supporting one hundred terminals should give response time of less than two seconds, evaluation of this aspect of system operation can be done easily after the system becomes operational.

Information evaluation:

An information system should also be evaluated in terms of information it provides. This aspect of system evaluation is difficult and it cannot be conducted in a quantitative manner, as is the case with development and operation evaluations. The objective of an information system is to provide information to support the organizational decision system. Therefore, 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 is practically impossible to directly evaluate an information system's support for decision making in an organization. It must be measured indirectly. There is an approach based on the concept that the more frequently a decision maker's information needs are met by a system, the more satisfied he tends to be with the system. Conversely, the more frequently necessary information is not available, the greater are the efforts required obtaining the necessary information, and hence, there will be greater dissatisfaction with the information system. Thus, satisfaction can be used as a measure to evaluate the information provided by an information system. Measurement of user satisfaction can be accomplished using the interviews and questionnaire technique discussed earlier. If management is generally satisfied with an information system, it is assumed that the system is meeting the requirements of the organization. If management is not satisfied, modification ranging from minor adjustments to complete redesign may be required.

SYSTEMS MAINTENANCE

Most information systems require at least some modification after development. The need for modification arises from a failure to anticipate all requirements during system design and/or from changing organizational requirements. The changing organizational requirements continue to impact most information systems as long as they are in operation. Consequently periodic systems maintenance is required for most of the information systems. Systems maintenance involves adding new data elements, modifying reports, adding new reports, changing calculations, etc.

Maintenance can be categorized in the following two ways:

1. Scheduled maintenance is anticipated and can be planned for. For example, the implementation of a new inventory coding scheme can be planned in advance.
2. Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate solution. A system that is properly developed and tested should have few occasions of rescue maintenance.

One problem that occurs in systems development and maintenance is that as more and more systems are developed, a greater portion of systems analyst and programmer time is spent on maintenance. An information system may remain in an operational and maintenance mode for several years. The system should be evaluated periodically to ensure that it is operating properly and is still workable for the organization. When a system becomes obsolete i.e., new opportunities in terms of new technology are available or it no longer satisfies the organization's needs, the information system may be replaced by a new one generated from a fresh system development process.

CHAPTER 11

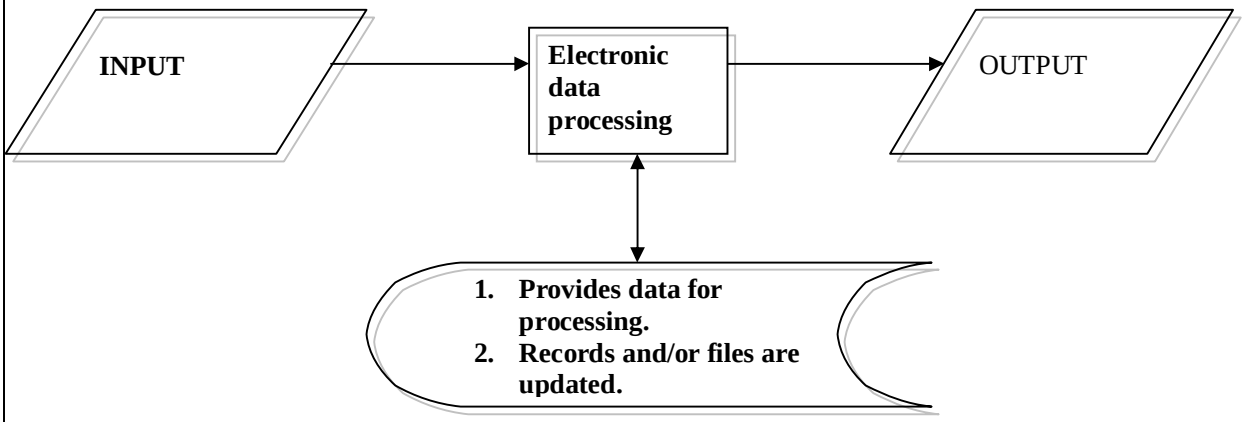
DESIGN OF COMPUTERISED COMMERCIAL APPLICATIONS

The purpose of this chapter is to introduce the students to accounting information systems applications. These applications are discussed in this chapter by means of flowcharts.

We have chosen batch processing system to explain these applications, though in future, on-line systems will be more common. The transactions in these applications are entered on floppy diskettes, processed periodically against the master files to produce the desired reports, summaries, projections etc. in a computer step (also known as the computer run). These transactions may have to be sorted before the file updating run, by the key in which the master file has been arranged using sort utilities. The floppy diskette has been used for the transaction files and magnetic disk/tape has been used for the master files.

General form of business applications

The chart shows the general form of business applications. It emphasizes that all the outputs are prepared from the inputs (transaction and master files).



INPUT
1. Transaction data Source documents online input
2. Database adjustments adjustment documents online adjustments and inquiries
3. Output of other systems

OUTPUT
1. Reports
2. Documents
3. On-line responses and displays
4. Control listings
5. Input to other systems.

ACCOUNTS PAYABLE

The purpose of accounts payable computer system is to pay for goods or services received from vendors. Most services and supplies are purchased “on account”, rather than by cash payment at the time of purchase. Therefore, a number of unpaid invoices accrue to a vendor. Prompt payment of outstanding invoices can be very important to the vendor, since money is needed to satisfy the vendor’s creditors. To encourage payment, most commercial vendors allow their customers cash discount for paying the bill or invoice within a specified time. A cash discount is usually 2% of the total bill, although it can be more or less. Vendors also attempt to collect interest for late payment as another method of forcing prompt payment. However, this practice is usually not very successful;

Initial Input to the Payable System:

The initial input to the accounts payable are batches of invoices supplied by the accounting department. When material is purchased, a number of documents accompany the purchase of material from a vendor. Since every vendor may submit a different form of invoice, payable forms vary considerably in size, layout, information contents and readability. Therefore, it is a common practice to extract by hand vital data from the each invoice and record this information on a standardized disbursement voucher. This disbursement voucher stapled along with the invoice it represents, is sent to the data entry department for input of data.

Input to daily processing of vendor invoices consists of

-Accounts payable disbursement vouchers
-Batch control record and
-Vendor change records.

This system uses two input files namely

-Vendor master file and
-Accumulated accounts payable file produced by the daily processing run.

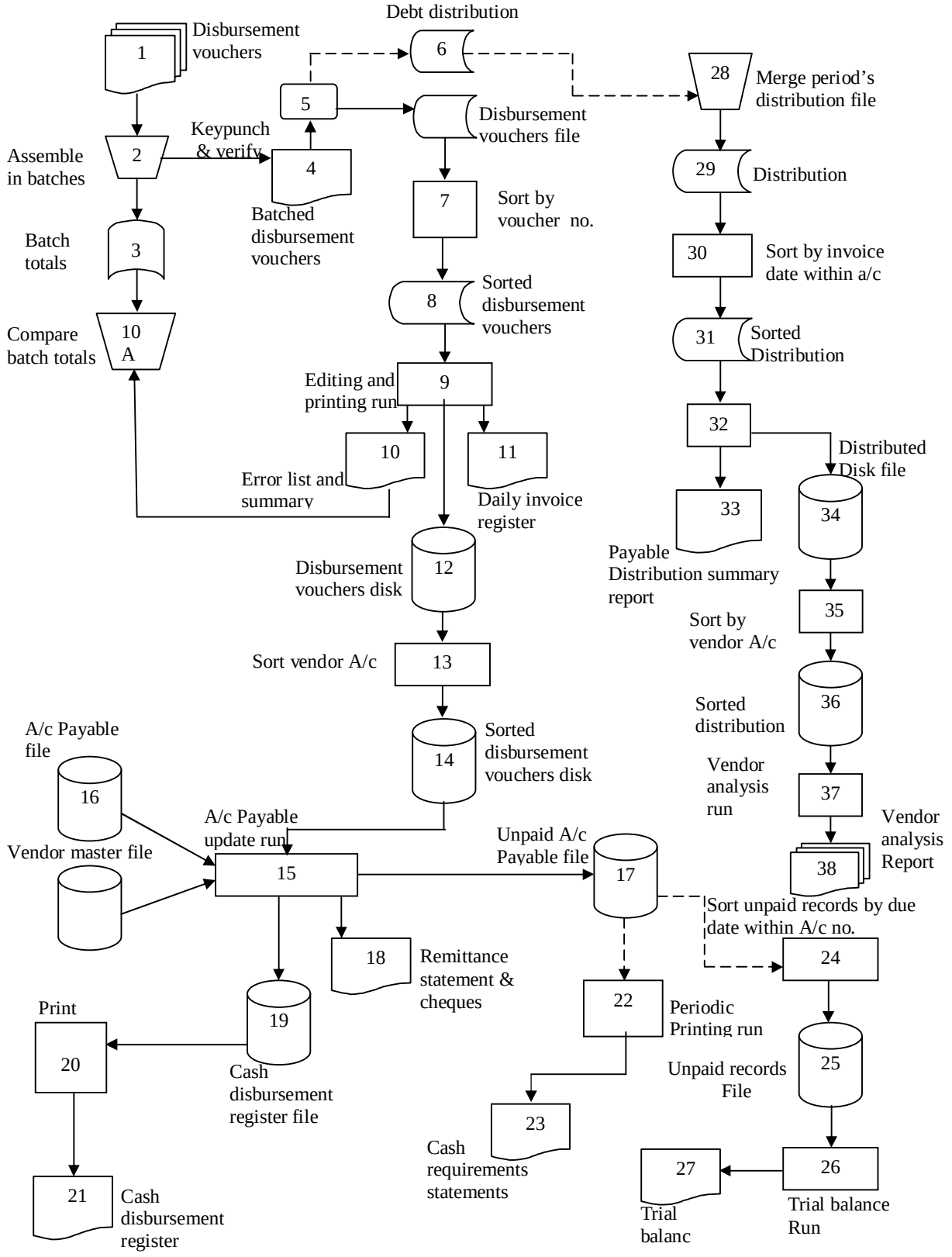
Both of these files are updated during daily processing invoices.

Various outputs produced by this system are

-Daily Invoice register
-Cash disbursement register
-Remittance statement and cheques
-cash requirements statements
-Payable distribution summary
-Vendor analysis reports

Explanation to various runs shown in figure:

1. The purchasing department receives the invoices from the vendors. After verifying and editing each of these, it prepares a disbursement voucher for it by assigning the voucher number serially and the vendor A/c number.
2. The disbursement vouchers for the day are assembled in a batch.
3. The following batch totals are derived on an adding machine.
   (a) Record count i.e. the number of disbursement vouchers in the batch.
   (b) Hash total of the vendor A/c numbers.
   (c) Financial total of the net amount data field.
4. The batch of the disbursement vouchers headed by the control totals slip is forwarded to the computer data processing department.
5. In the data-entry section, for each disbursement voucher, a disbursement voucher record is prepared on the data-entry machine as also as many debit distribution records as the number of items lines are prepared on the data-entry machine. The records are verified also. The verified records are stored on a floppy disk.
6. The disbursement voucher records are sorted by the voucher number as the key.
7. It gives the sorted transaction file of disbursement voucher records on a floppy disk.
8. Editing and Printing Run. Various checks are applied to the disbursement vouchers transaction file. Those transactions that fail to clear these checks are printed in the error list (10) on which are also printed the batch totals as the summary information as derived by the program in this run. The daily invoice register is produced as another output(11). The disbursement voucher data is put into magnetic disk/tape (12) for subsequent speedier processing



Accounts Payable Application

10. (A) Error List and Summary Information compared with the batch totals derived on an adding machine prior to computer processing. Also the erroneous transactions are investigated in the purchasing department. These would be resubmitted for processing after rectification.
13. The disbursement voucher disk/tap (12) is sorted by the vendor A/c no. in this run and gives the sorted disbursement voucher disk/tape (14) as its sole output
15 A/c Payable Update Run. The A/c Payable file (16) along with Vendor master file is updated in this run by the disbursement vouchers disk/tape (14).

The program scans each vendor record for those pending disbursement vouchers for which payment is due today, prints cheques and remittance statements for them, and deletes them from A/c Payable File (16). The new disbursement vouchers are added to their respective vendor records. This run yields the following outputs:

A/c Payable file C/F (17)
Remittance Statement & Cheques (18)
Cash Disbursement register disk/tape file (19).

20. In this computer run, the cash disbursement register (21) is obtained as the output.
22. in this periodic (weekly, perhaps) run, the A/c payable file is used to produce the Cash Requirements Statement(23).
24. In this run which is carried out at the end of each accounting period, the unpaid records on the A/c Payable file are extracted, sorted and put on disk/tape as the unpaid file (25).
26. From the unpaid records files (25) the trail balance (27) is derived in this run and printed.
28. At the end of the A/c period all the distribution records are merged in one file (29).
30. The distribution record file is sorted by the invoice date within the A/c number to obtain the sorted file of distribution records (31).
32. In this computer run, the A/c payable Distribution Summary is printed(33)
35. In this run, the distribution records (34) for the period are sorted by vendor A/c no.
37. The sorted distribution record disk/tape (36) is used in this run to produce the various vendor analysis reports (38).

PAYROLL ACCOUNTING

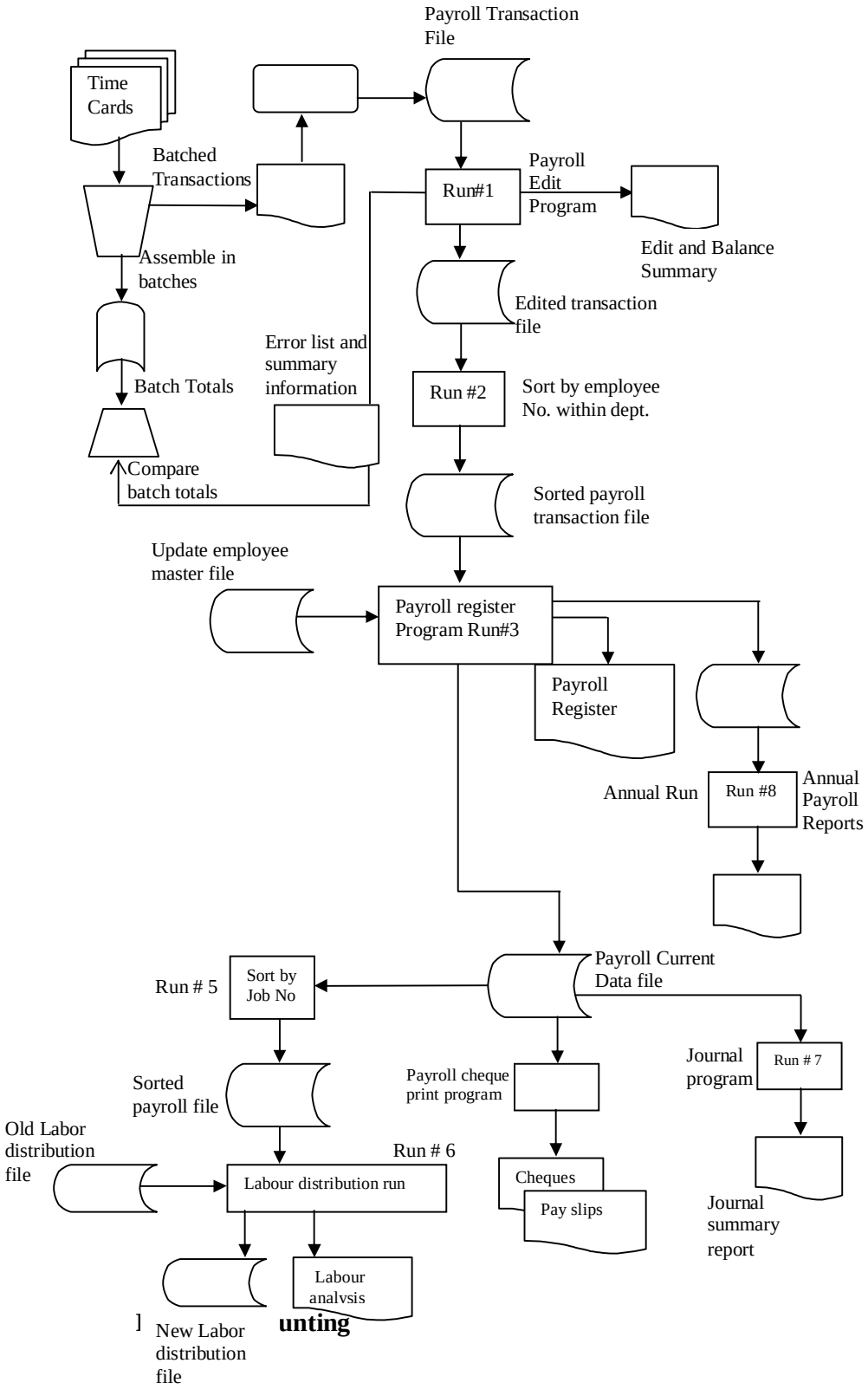
Payroll is one of the oldest and most common business computer applications. A decade or two ago, company payroll were frequently computed using calculators and then printed by tabulating machines. The basic purpose of the payroll system is to produce payslips and pay cheques for the employees every month.

Preparing a payroll requires collecting employee work hours through their attendance cards, converting hours to gross earnings and computing deductions and the pay. Of course, there are other activities to be performed as by products of payroll operations. These includes accumulating summary data for general ledger reports, printing quarterly and year-end reporting statements, and making labor distribution and job costing or job performance measurements and reporting them. In addition to accounting activities, a payroll system commonly performs activities that might be viewed as personnel operations: sick leave and earned leave accrual and usage, and home address maintenance. While these activities enlarge the size of computer records for payroll operation, they do not significantly increase the complexity of managing the overall operation.

Input files

Master file: the payroll computer application is one of several business systems that can be processed using a combination of current and year-to-date master computer file. This file consists of records for the current reporting period as well as for yearly reporting. The master file also contains permanent and current data.

The permanent portion of the file must be updated before current transactions are entered into the system, since information such as employee's rate of pay; accumulated earned leave, change in status code etc. are used to transform gross salary into net pay. Therefore, prior to actual processing of a payroll, a preliminary master file update must be completed.


Payroll Transaction File
Time Cards
Batched Transactions
Run#1
Payroll Edit Program
Edit and Balance Summary
Assemble in batches
Edited transaction file
Error list and summary information
Batch Totals
Run #2
Sort by employee No. within dept.
Compare batch totals
Sorted payroll transaction file
Update employee master file
Payroll register Program Run#3
Payroll Register
Annual Run
Run #8
Annual Payroll Reports
Payroll Current Data file
Run # 5
Sort by Job No
Journal program
Run # 7
Sorted payroll file
Payroll cheque print program
Old Labor distribution file
Run # 6
Labour distribution run
Cheques
Pay slips
Journal summary report
Labour analysis
New Labor distribution file

Payroll master file update

Before time cards are submitted at the end of a pay period, the accounting department obtains data on new employees and on recent changes to existing employees such as correct spelling of name, change in address, marital status, pay scale, overtime rate, rates of sick leave and earned leave, change in department employed by and an employees number.

New employee information is submitted to the data entry department on a payroll change input form. These forms contain space for all vital data to be entered into the system. Keyed employee additions and changes update the most recent version of the payroll master file. It may be noted here that copies of master file should be retained before and after updating. Thus, if an error is found, it can be corrected and updating can be repeated. An employee change report is also printed as a result of this update run. It is convenient if the change report is printed in the same sequence as the input documents, since the report can then be edited manually without searching for the corresponding change input form.

Input to the Payroll Application

After changes to the payroll master file, the actual payroll run begins. Time records are submitted for data entry. The information contained in these time cards is entered in the form of a transaction file. Batch control totals for various fields are computed. This batch control information is keyed to a lead record (the first record is a batched set of records for payroll input). Lead record information is used by the computer to check the accuracy and completeness of the batch of payroll records.

Processing of the payroll system

Given figure shows the processing of payroll. Inputs to the system consists of keyed data for time cards, batch control information, and the employee master file, updated by the preliminary master payroll file update. Outputs from the system include a completed employee master file, updated by time cards information, and the reports and documents discussed below:

In run#1: The payroll edit program is executed. The first function of this program is to detect errors in the input data (for example, invalid employee number, excessive hours worked, or an hourly employee showing no regular hours worked). If an error is detected, it is immediately printed to permit correction. If accumulated totals computed by the computer program from individual records do not balance control totals contained on the lead record, the difference is also printed. Processing is discontinued at this point so that errors can be corrected. Once this is done, the edit program is return to produce an error free input file. The input file produced by the payroll edit program is recorded on magnetic disk or tape.

In run#2: The payroll transaction file is sorted by the employee number within department number.

In run# 3: The sorted transaction file is used to update the master file on magnetic disk. The type of code stored in master file indicates the nature of the account to which employees' gross pay is charged such as direct labor, indirect labor etc.

Gross and net pay are calculated in this run; year-to-date and current period data are accumulated and written on the payroll master file. The data necessary for printing payslips and pay cheques for the current period are put on a magnetic tape/disk constituting another output of this run. Payroll register is also printed during this run. Payroll register is a printed record of details in the completed employee master file.

In run # 4: The current period payroll master tape/disk is used to produce pay cheques and payslips.
In run # 5: The current period payroll tape/disk is sorted by job number.
In run # 6: The output file of Run#5 is used to update old labour distribution file.

The cumulative values of various trades as at the end of last month are updated to as at the end of this month by means of the payroll file.

This labour analysis is printed for each job as another output of this run.

In run # 7: A journal report is printed. This report is used to supply current and year-to-date entries to the general ledger, which is the final consolidated accounting document. Journal reports record total funds expended by source and by disposition. For example, total money amount for overtime and total amount for special advances etc. are summarized by separate account on the general ledger. Similarly, total insurance premium deductions, provident fund deductions, staff welfare fund, income tax deduction etc. make up other accounts.
In run # 8: The completed master payroll file is used to print quarterly/annual reports. Government regulations require quarterly/annual reports on payroll activities. Such reports include provident fund deduction statement, income-tax deductions, insurance premium deductions etc. many other reports for internal accounting purposes may also be printed on quarterly/yearly basis.

FINISHED GOODS INVENTORY CONTROL

Traditionally, the inventory carried by a firm serves as a buffer for stages of production. Thus, inventory management may 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. With the advent of the computer, the management of inventory has taken on a new dimension based on viewing inventory as an investment. As it often consumes a high proportion of working capital, it must be controlled in the most effective manner.

General design of inventory system

Input files

Inventory system generally requires the use of several data files. The basic file of this application consists of an "inventory master file" which keeps track of the quantity of each item available in stock. In addition, it also gives information regarding the location of each item in the warehouse, the cost of the item, the reorder point, the quantity currently on order, name and address of the vendor from whom the item is purchased, and the historical data.

One transaction file is maintained to keep track of individual sale transactions: to which vendor items were sold, when, for what price, and the invoice or receipt number. A second type of transactions contain data describing stocks received by the receiving department of the business firm. Input may also include "miscellaneous inventory transactions" such as adjustments for lost or damaged stock. Using the transactions files, the master file is continuously updated to reflect changes in the inventory level caused by filling sales orders or receipt of new stocks. A "back order file" is also updated for sales orders that can not be filled because of stock outs. Some customers are willing to wait until new stock is received. The back order file provides data on outstanding back orders that must be filled when stock receipt notices are received for back-ordered items.

Outputs From The System

The outputs of the inventory control system includes the following:

1. The inventory transactions listing for control purposes.
2. Inventory ledger
3. Customer's report
4. Back-orders file
5. Excess-stock
6. Under-stock
7. Slow-moving
8. ABC class items
9. Items-to-be ordered file

Data describing filled orders, back-orders and miscellaneous sales order transaction is major systems output and becomes the primary input into the billing and sales analysis system. Information concerning back orders, out-of-stock items, reorder points; economic order quantity is sent to the purchasing or production department for entry into their information system. Various exception reports analyse inventory status in order to help management to meet the objectives of inventory control.

Run Flowchart

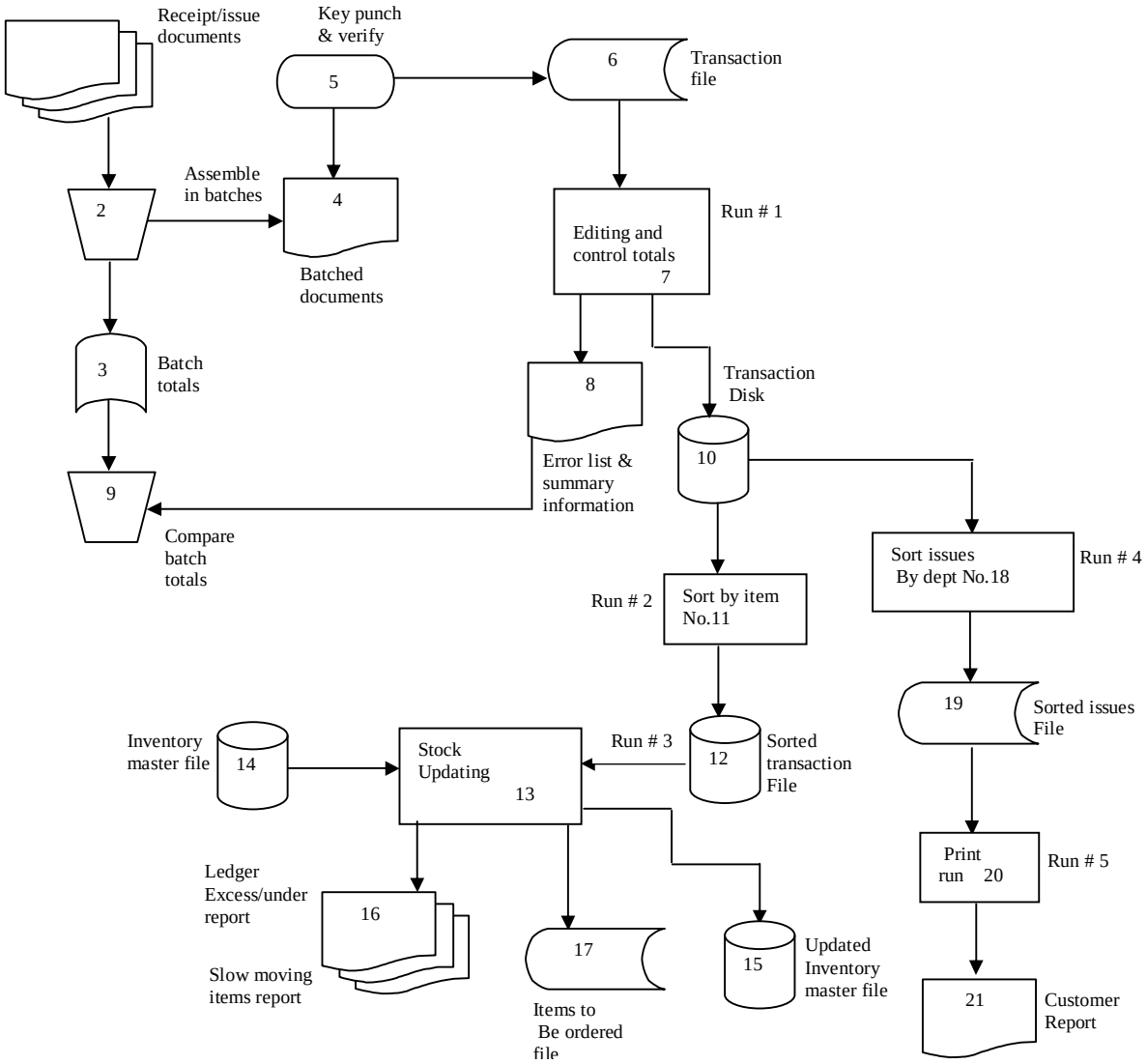
This application on hand requires 5 runs. Each run has its own program and is performed in a computer set up after loading this program in the computer memory. The run flowchart for the application on hand is shown in the figure. The symbols in it are numbered from 1 to 21 to facilitate the following explanation:

1. The receipt and issue notes are prepared in the stores department as and when these transactions arise. It is desirable that the format of such source documents are so designed that they facilitate transcription of data from them into computer media. Also the receipt and issue notes may have different colours. The notes in a pad should be serially numbered to keep track of each of these.
2. The receipt/issue notes for the day are assembled in batch.
3. The following controls totals for the batch are derived on an adding machine, perhaps:
    1. Record count, that is, the number of notes in the batch.
    2. Hash totals of the item numbers.
    3. Financial total of quantities received and issued.
4. The batch of the receipt/issue notes along with the control slip bearing the batch totals is transmitted by the stores department to the data preparation section.
5. A record is prepared for each transaction. The records are also verified on the data entry machine by an operator who is different from the keypunch operation and who uses the same source documents (goods receipt notes and issue notes).
6. This transaction file is used as the input to run # 1.
7. In this run editing is performed on the transaction records. A couple of the possible checks that can be performed are:
    1. Check digit on the item code, and
    2. Date check.

Those control totals which were derived manually prior to processing are now derived by the program. The Error List and Summary Information (8) lists the erroneous transactions and also the control totals. These totals are then checked (9) with their opposite numbers derived manually (3) prior to processing. If they do not tally, investigations for the accidental/fraudulently motivated reasons would be under taken also. The Error List would be forwarded to the stores department to scrutinize the erroneous transactions, rectify and resubmit them for reprocessing. The corrected transactions file is output on a magnetic disk for subsequent speedier processing.

9. In this run, the transaction disk file (10) is sorted by the item number as the key to give the sorted transaction file (12).
13. In this run, the sorted transaction files is used to update the inventory master file on magnetic disk.

    Items to be ordered file (17) containing particulars of those items for which the stock level has fallen below the reorder. This file may be used in another routine to produce purchase requisitions or orders; but that was have not included this application for the time being.



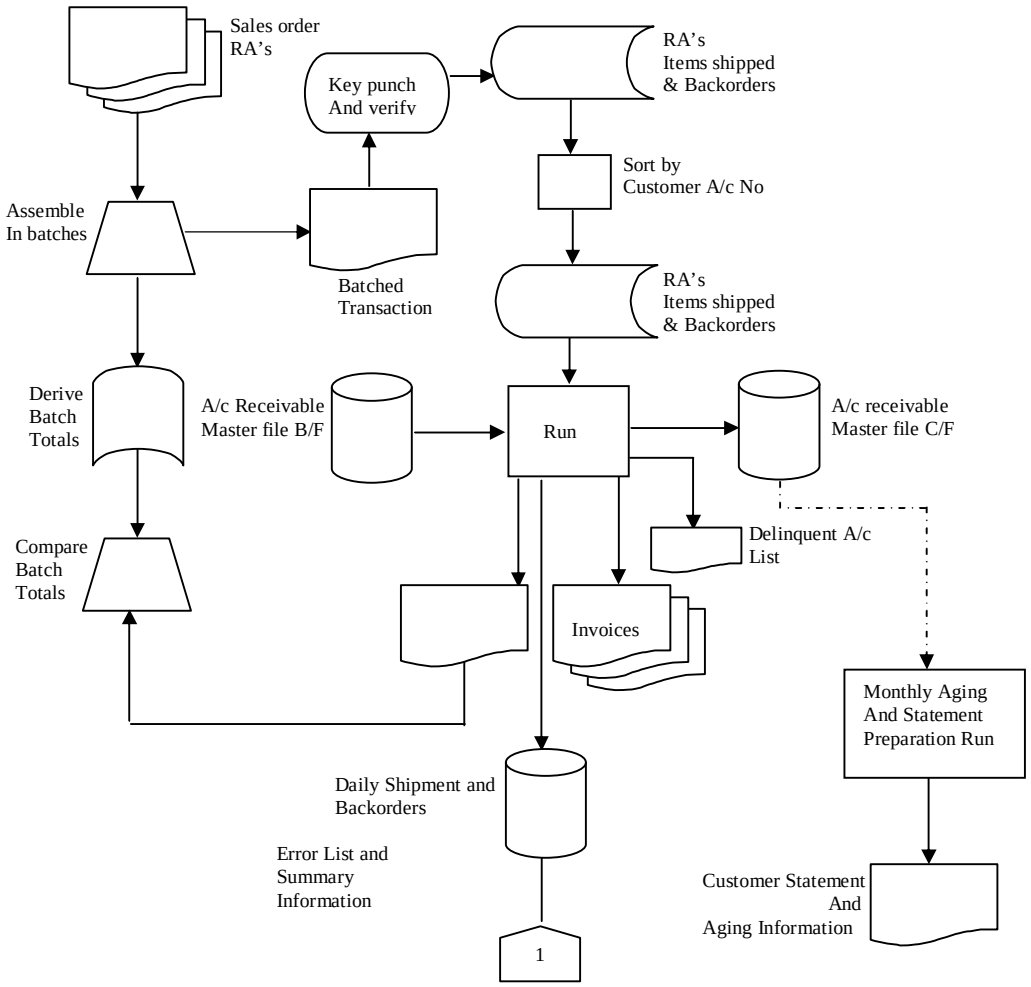
Finished goods inventory control

18. The transaction file for the period are merged, receipts ignored and sorted by the department number in run 4 to give the sorted issues file (19).
20. In this run the sorted issue file (19) issued to produce the printout of the customers report (21).

SALES ORDER PROCESSING SYSTEM

The sales department prepares the sales orders, in duplicate upon receipt of the custormer's purchase order or telephonic information from a salesman or the customer after satisfying themselves that the customer's account is not delinquent. One of the outputs of a computer run to be discussed subsequently is the list of delinquent accounts which the sales department consults to establish credit worthiness of the customer. One of the copies of the sales order is sent to the customer as an acknowledgement of the receipt of his purchase order. The other copy is sent to the shipping department as an authorization to ship the goods to the customer. The format of the sales order should be so designed that also transcription of data from it on to floppy disk subsequently. The sales department enters the quantity shipped and quantity back ordered against each line on the order, i.e., for each stock item on order, the price having already been entered by the sales department. The shipping department assembles the sales order in daily batches and compiles the following batch

totals for it on an adding machine, perhaps: record count, financial total of the values of items shipped and hash totals of quantities shipped, quantities back ordered, customer's account numbers and stock item numbers. The batch of the sales orders together with the control slip bearing these batch totals is then forwarded to the data processing department for transcription on the floppy disk.



Sales Order Processing System

Likewise, the mailroom assembles the daily batch of remittance advises received from the customers and compiles the following batch totals for it: record count, financial total of the amounts remitted and the hash total of the customer account numbers. The batch together with the control slip bearing these totals is forwarded to the data preparation section.

We are dealing with only two types of transactions of this application for simplification of illustration though in practice there would also be the following inputs:

1. addition of new records to the file
2. credits for sales returns and allowance
3. account right-offs
4. Change of addresses and other routine adjustments and corrections.

The data preparation section of the data processing department records data on floppy disk for each item back-ordered, each item shipped and each remittance advice on the computer. This floppy disck is then given to the verifier operator who verifies the records by re-entering the transactions data. For economies in verification time, it may, however, be desired that just the critical data files on the records are verified.

These verified records are then sorted using SORT utility with the customer account numbers as the key.

The sorted file constitutes the transaction file which is used to update the accounts receivable master file by the account receivables update program in computer run. In this run, customer accounts are updated for the sales.

The outputs of this run are as follows:

1. The updated A/c receivable master file.
2. Delinquent accounts list which contains the particulars of those customers who have crossed either the credit limit or the credit rating assigned to them.
3. Invoices in as many copies as desired. It has to be noted that invoice would be prepared for only the items shipped.
4. Daily shipment and back-orders file: the data stored on floppy disc is put on to magnetic disk for a subsequent speedier resorting by stock item number as well as speedier processing against inventory file the discussion on which would follow.
5. Error list and summary information: this contains the rejects i.e., those transactions which could not pass the control checks. These are ultimately investigated by the user department, rectified and re-submitted to the data processing department for re-processing. The summary information consists of all the batch totals derived by the computer. These batch totals are compared with the ones derived manually prior to processing and entered into control slips travelling with the batches of the transactions.

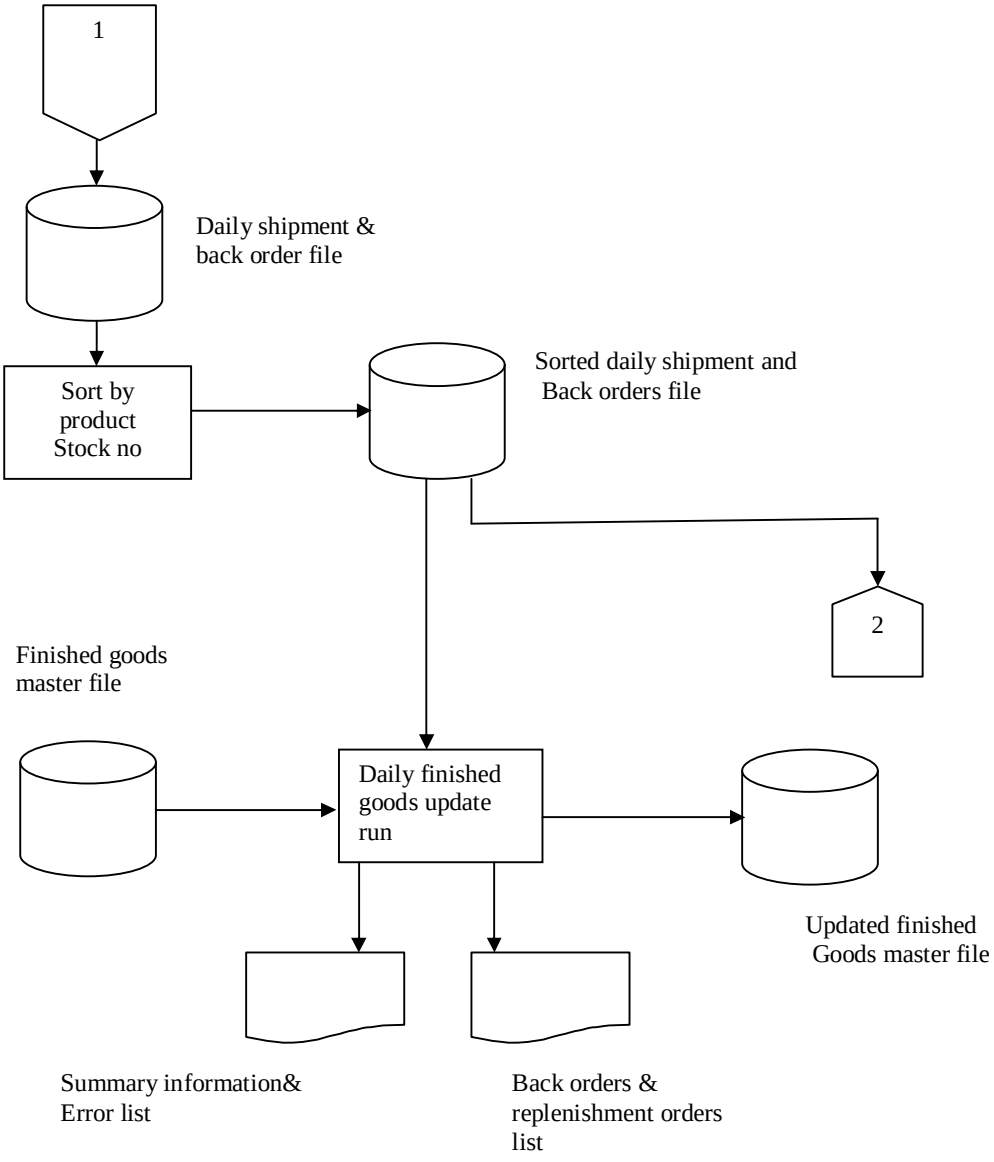
The accounts receivable file is also processed every month to produce the customer statements and aging schedules.

Linkage with inventory processing application: The daily shipment and back orders file obtained as an output of a run in the previous flowchart can be used to update the finished goods master file according to the concept of integrating various business applications. Since, however, the finished goods master file is sequenced by the product stock number as the key, the daily shipment and back-orders file is also sorted in this order. In the daily finished goods update run, sorted daily shipment and back-orders file constitutes the transaction file and by updating finished goods master file, the system produces the following output:

i. Finished goods master file is updated for the various stock balances in it. Back order-sub-records may also be added.

ii. Back-orders and replenishment orders list: the items for which the stock balance has fallen below the reorder level would find place in the replenishment orders list. “Backorder” means a customer’s order for an item against which goods cannot be supplied now but would be supplied as and when they are received from the works.

iii. Summary information and error list: the summary information consists of the various batch totals derived by the computer. These will ultimately be compared with their counterparts derived manually prior to computer processing. The error list would contain erroneous transaction which could not pass the various checks build in the computer program.



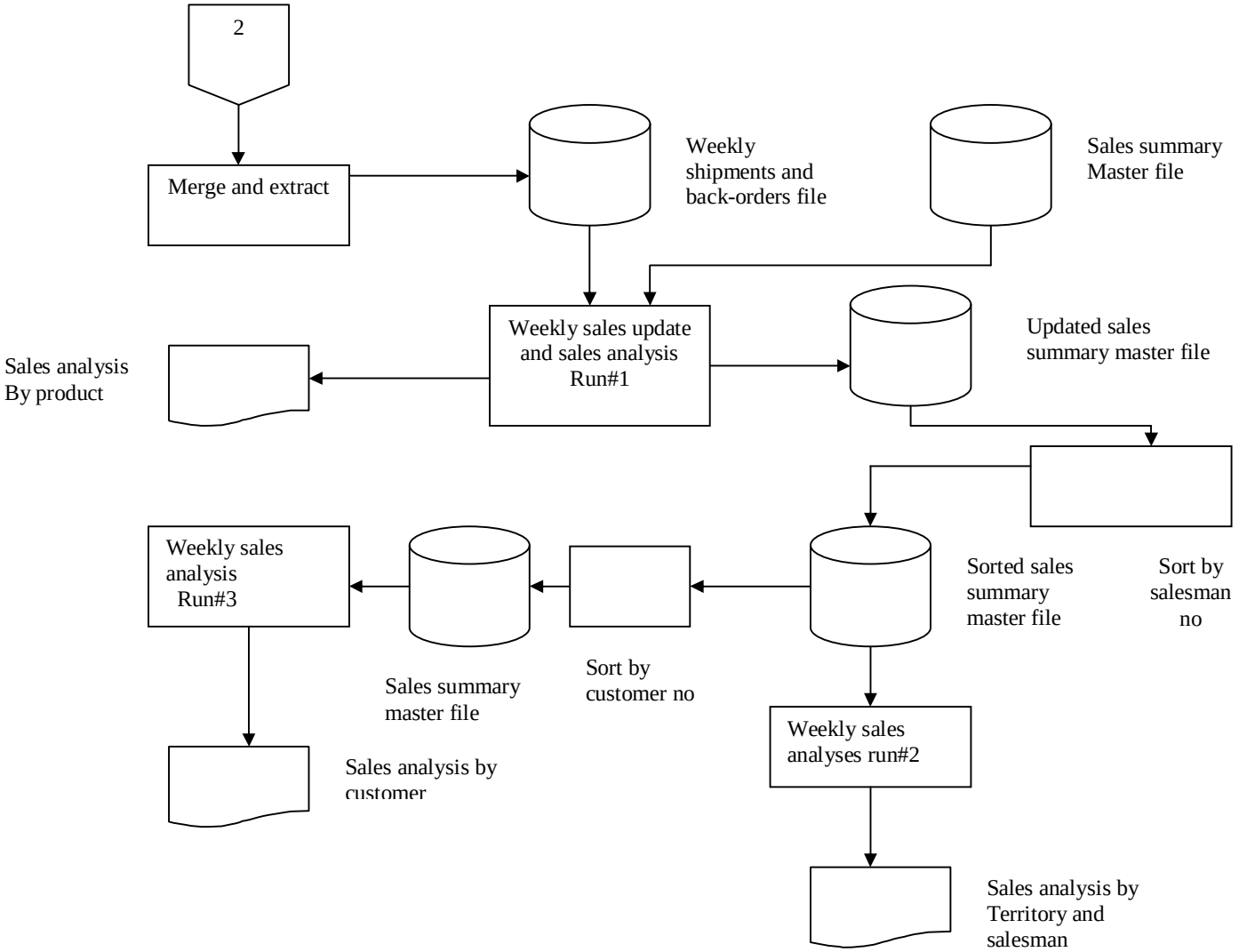
The sorted daily shipment and backorders file in consonance with the concept of integration, is used in the following flowchart for sales analysis runs.

SALE ANALYSIS RUNS

The sales analyses are made by updating the sales summary Master File by the daily shipment and back orders file.

It is assumed, however, that to start with, the sales summary master file is sequenced by the product stock number and, therefore, it is straightway updated in run 1 by the daily shipment and back-orders file. As an output, the sales analysis report by product stock number is obtained.

The sales summary master file is then sorted by the salesman number as the key and in run # 2 a printout of the sales analysis by salesman is obtained.



Sales Analysis Run

The sale summary master file is finally sorted by the customer number as the key and in run #3 a printout of the sales analysis by customer is obtained.

So far we have discussed various computerized business application under batch processing mode merely for illustration. However, in practice, the trend is towards development of these applications in an interactive and on-line mode. Most of these micro-based software packages are interactive and menu-driven. They provide facilities for on-line entry of transactions and master files, validation of input data, creation of various analysis and summary reports and exception reporting for management requirements. We have given below an example of an on-line, real-time sales order processing system. Subsequently we have discussed a number of applications which are integrated, in the same that output of one application may be used as input to another application.

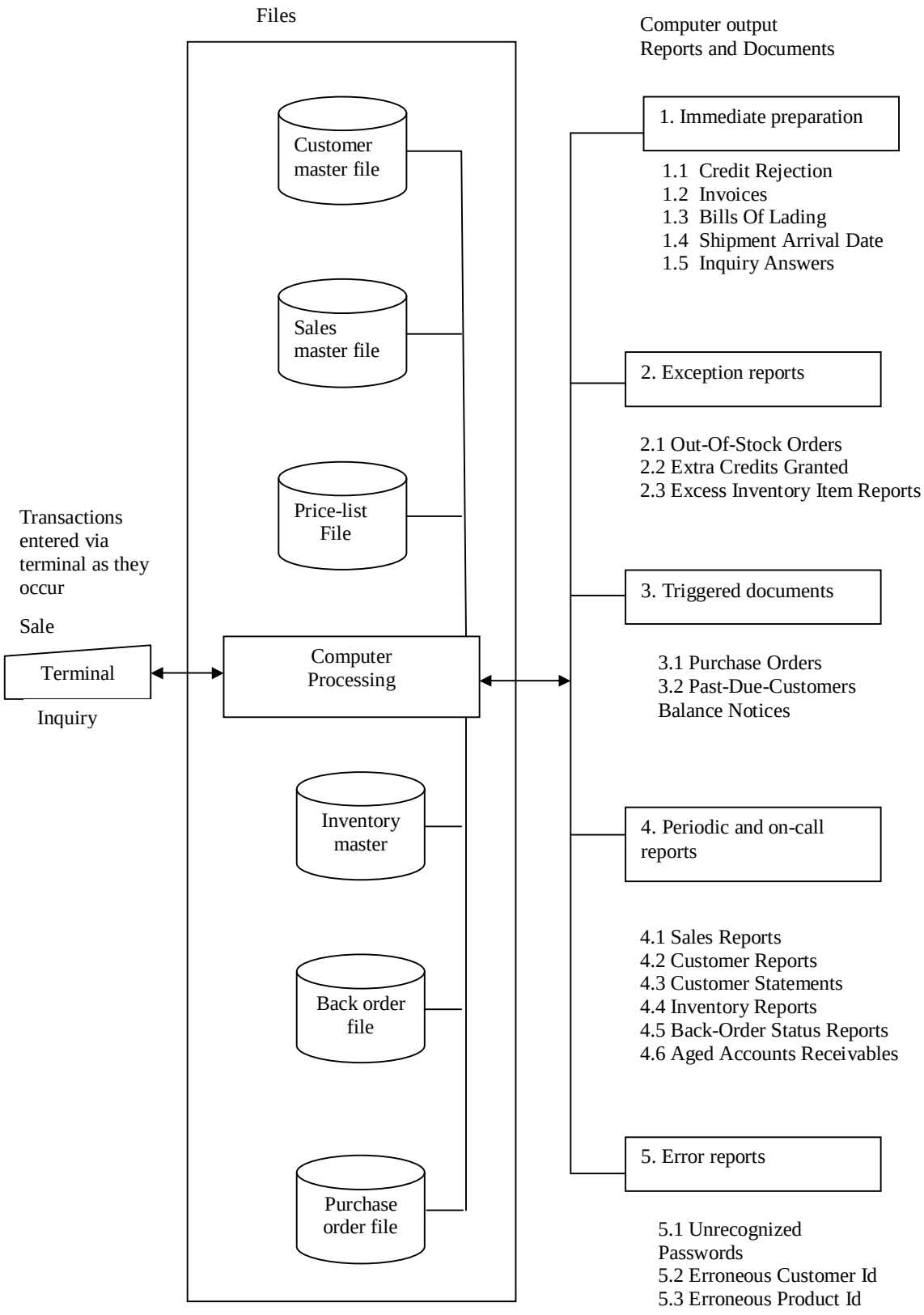
THE SALES ORDER PROCESSING SYSTEM:ON-LINE, REAL-TIME

An on-line, real-time (OLRT) sales order processing system can fully process a transaction as soon as it is entered; thus no delays occur during computer processing. When coupled with a point-of-sale (POS) transaction recording and entry system whereby the transaction is initially recorded in machine-readable form and entered directly into the computer, the system is fully automated, and even the delay in entering the transaction is eliminated.

In an OLRT system, all files of the subsystem related with a particular type of transactions processing must be electronically connected to the computer when a transaction of that type is entered into the computer. For technical reasons, the files of an OLRT system must consist of magnetic disks. Given below figure shows six disk files, each containing accounts or other information that the computer programs can access immediately.

The OLRT system illustrated operates in a totally different manner from the way batch systems do. Assume that customers order by telephone and that the salesperson who receives customer's orders immediately keys the transactions at a terminal. Controlled by the sales order entry computer programs, the following events occur immediately in the sequence given below for each transaction:

1. The sales person tells the computer the nature of the transaction by entering a transaction code identifying it as a credit sales transaction; this activates the sales order processing computer programs. The customer number, the item number and quantity are then entered.
2. The computer program checks the customer's account in the customer file to "validate" the customer number (to establish that a credit customer exists with that number) and to see how much additional credit the customer can be granted; the up-to-date credit status of the customer is contained in the customer's account. If the customer cannot be extended further credit, the salesperson is notified by the computer and the credit transaction is cancelled.
3. The product number of the product ordered is checked for validity in the inventory file, and the stock level of that item shown by the inventory file is compared with the number of items ordered. If there is an insufficient quantity of a product, the program examines the purchasing file to establish when the next shipment is due. The system conveys this information to the terminal of the salesperson and awaits further instructions. The salesperson consults with the customer and then cancels the order for that item or changes the order to the quantity available and back orders the additional items desired, according to the customer's wishes.
4. The computer program then seeks product pricing and quantity discount information from the price list file and special "preferred customer" discount information, if any, from the customer file. The total cost of the item to the customer, including tax, is calculated by the computer.
5. The details of the transaction, including the cost details, may appear on a display device at the salesperson's terminal so that they can be told to the customer. Changes may be made in the order by the customer and entered into the computer. The salesperson signals the computer when the customer approves the transaction.
6. An invoice is printed out for mailing, either at the salesperson's terminal or on a printer at a central location.



OnLine-Real Time Sales Order Processing System

7. On a printer at the warehouse location of the merchandise, the computer system prepares a multipart shipping document, which is the authorization for shipping personnel to select, pack, and ship the merchandise ordered. One copy of the document, knows as the "bill of lading" is enclosed and shipped with the merchandise.
8. Product records in the inventory file are adjusted to reflect the decrease inventory caused by the sale.
9. The customer's account is updated to reflect the details of the transaction, and a new customer balance is calculated and placed in the account.
10. The record for each item in the sales file is updated with details of the transaction. This updating may include all details necessary for sales analysis based on customer type and territory, as well as other factors. A separate transaction listing that records all details of the entire transaction in one transaction file may also be made for control and backup purpose.

The transaction processing described above may occur within a matter of a minute or two after the transaction is originally entered, while the customer is still on the telephone. In an OLRT system, the records can be kept current on a minute-by-minute basis. Inquiries from customers about the details of a recent transaction, about account balances, or about quantities of a product that are available for sale can be entered through terminals and receive almost instant responses. If the price list file and the purchase order file are also receive almost instant responses. If the price list file and the purchase order file are also maintained on a current basis, inquiries about prices and expected arrival dates of shipments can be answered promptly.

Additionally, transactions can be rejected immediately if the customer is not eligible for credit or if the item ordered is out of stock. With a batch system, neither credit eligibility nor product availability may be known for a day or more after the order is received. Common errors in batch systems, such as the entry of an incorrect customer number or an erroneous product number, may require days to detect and even more time to correct. With an OLRT system, such errors are usually detected and corrected immediately.

Each of the reports shown in the above figure can be produced at any location desired. Typically, the credit rejection report, the inquiry answers, and the error report are displayed or printed at the terminal where the transaction is entered. Triggered reports occur when an internal condition automates a programmed algorithm. Such as when the quantity of an item on hand drops below a reorder level.

MATERIALS INVENTORY CONTROL

The 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 of inventory shortages. Therefore, it needs the following information to function:

1. The timing of purchases.
2. Whether materials received meet specifications and have been properly costing.
3. The status of inventory on hand.
4. The status of unfilled orders.
5. Anticipated demand.

Given figure depicts the flow of information to and from the materials inventory system. One of its major functions is to maintain a subsidiary ledger with accounts for each item in the inventory. This ledger should balance in total to the materials inventory control account contained in the general ledger.

System Interfaces

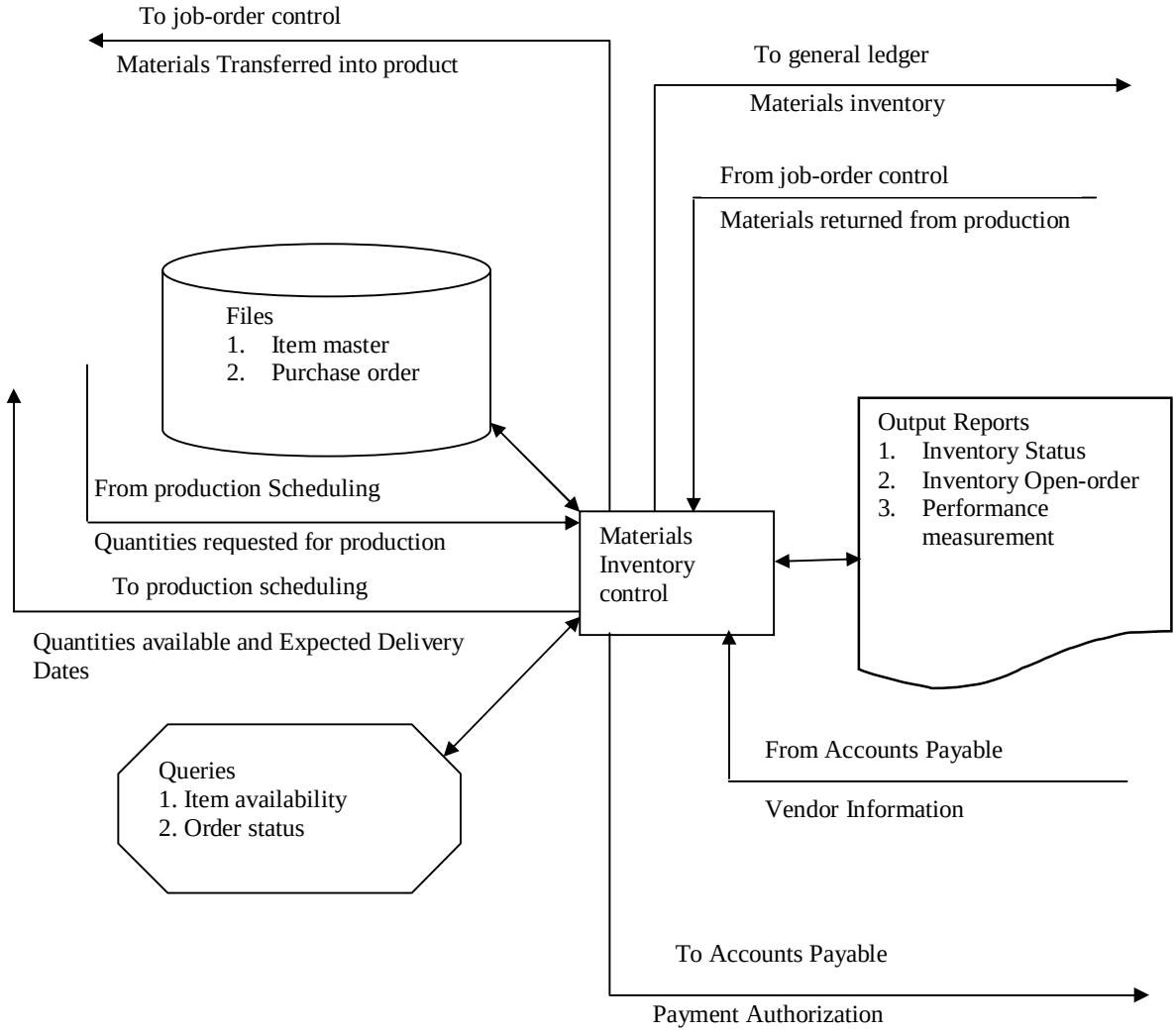
The materials inventory control system interfaces directly with the accounts payable, general ledger, work-in-process control, and production scheduling systems. Materials inventory control provides

accounts payable with information about vendors and the receipt of goods. Vendor information required when sourcing decisions are made. When an order is received, the materials inventory control system reports to accounts payable, which in turn, reports to authorize payment.

Materials inventory control provides the general ledger with certain accounting information. Specifically, the general ledger system needs to know the value of the purchases received, material transferred into production, and the inventory on hand. The aggregate journal entries generated and sent to the general ledger for the accounting transactions in the materials inventory control systems are:

The work-in-process control system contains the work-in-process accounts. Direct and indirect materials are requisitioned from the materials inventory control system and transferred to these accounts. On occasion, materials are returned from the production departments to materials inventory control.

Information concerning the quantities of items required for scheduled production is provided to the materials inventory control system from the production scheduling system. This information is used in determining order quantities and timing. In a similar way, information concerning quantities available and expected delivery dates is provided to the production to the production scheduling system by the materials inventory control system. This information is then used in scheduling production.



Material Inventory Control System

Files and inputs

Typical materials inventory control systems require at least two files. The item master file contains one record for each item in the inventory.

The item file is updated when a purchase order is created or items are placed in the inventory. Most queries of the materials inventory control system are for information contained in this file.

A purchase order file contains about new purchase orders. Purchase orders result from reduced quantities in the inventory or anticipated production requirements.

When materials are received into inventory, they are inspected and their quantity verified. Then the quantity and the cost based on the purchase order is sent to the accounts payable system to be used as a part of the data necessary to authorize payment.

REPORTS

On a periodic basis, the materials inventory control system produces at least some of the following reports. A inventory status report shows in the contains the quantities of each item available on a particular date. The unit cost is provided, and any costing technique [specific identification, FIFO, LIFO, average] can be used. Besides the ending balance, the beginning balance transfers, receipts, and adjustments are also included.

An open purchase order report contains information concerning the status of open purchase orders. It includes the items number, vendor identification, date of order, unit cost, quantity ordered, promised shipping date, and other status information. This report can be used to identify potential problems. For example, if a vendor misses a shipping date, cost estimation and production scheduling can be notified so that production schedules can be adjusted.

Performance measurement reports contain information concerning turnover, stockouts, shrinkage, investment, and other appropriate measurements related to management performance in inventory control.

WORK-IN-PROCESS CONTROL

The work-in-process control system assigns materials, labour, and overhead costs to production jobs or products. In a job-order system, each cost is assigned to a specific job. In a process costing system, costs are assigned to departments and then to products. The objectives of a work-in-process system are to cost jobs through the manufacturing process and provide management with information to assist in controlling cost and measuring the performance of departments or other units within the factory. Therefore, to function properly, the system needs information concerning [1] materials requisitioned for each job. [2] labour employed on each job,[3] overhead costs allocated to each job, and [4] the production status of each job.

System interfaces

The work-in-process control system interfaces directly with the payroll, general ledger, finished goods inventory control, production scheduling, and materials inventory control systems. Labour cost distribution and factory overhead allocation are inputs from the payroll and the general ledger systems, respectively. Aggregate work-in-process inventory transferred to finished goods in sent from work-in-process control to the general ledger. The aggregate journal entry is:

Once manufacturing is complete, jobs are transferred from work-in-process control to finished goods inventory control-that is, from the production management system to the marketing system.

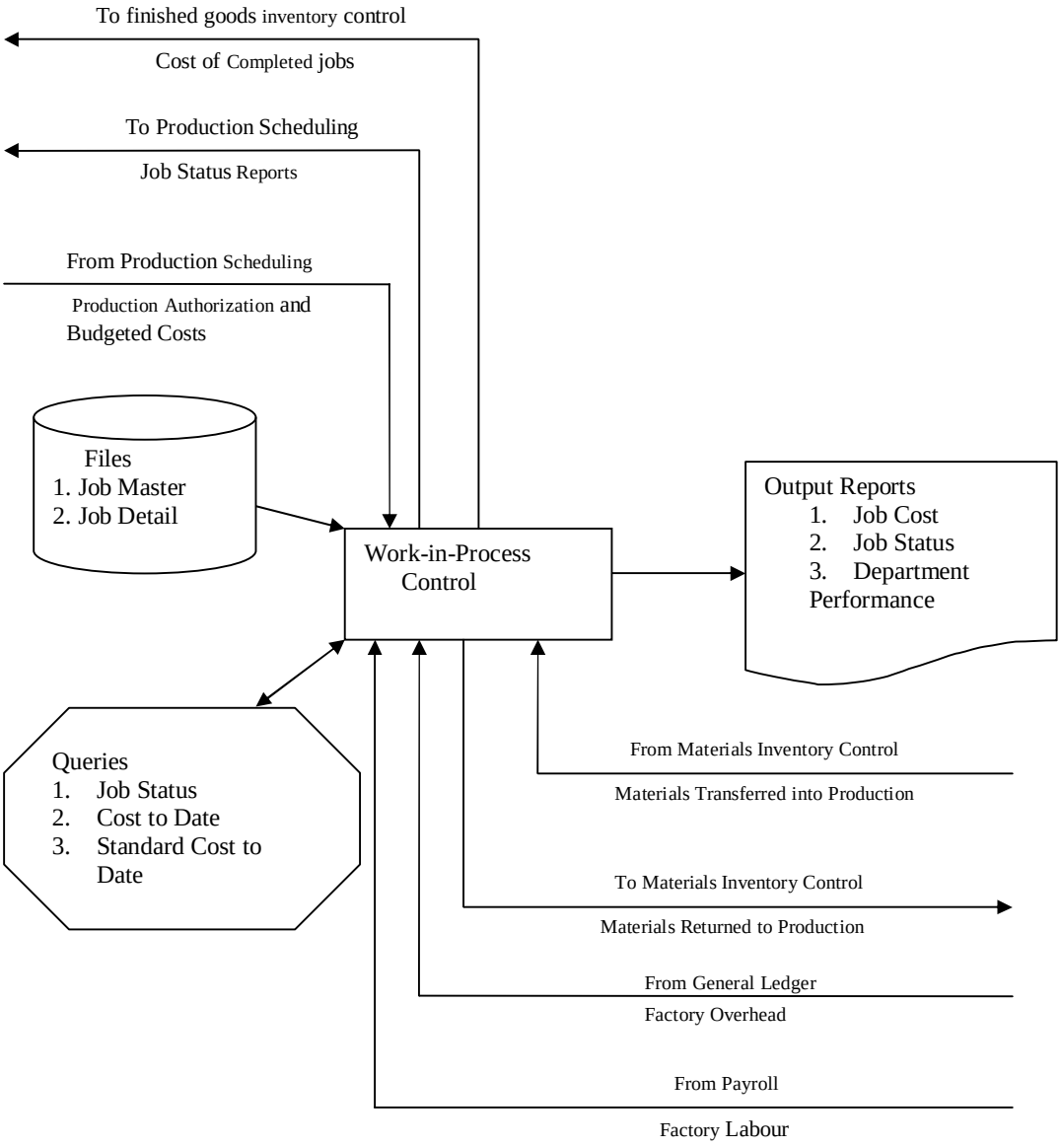
Authorization to start production along with a bill of materials, specifications, production schedule, and budgeted costs are transferred from the production scheduling system. Job status reports are

available to this system. Direct and indirect materials are requisitioned from the materials inventory control system.

Files and inputs

A typical work-in process system in a manufacturing firm contains a job file that has one record for each job in the manufacturing process.

The job detail file contains in-depth information about each job. When authorization to start a job is received from production scheduling, a record is created for the job. A bill of materials a machine schedule, and a labour schedule are entered into the file.



Work-in-Process Control

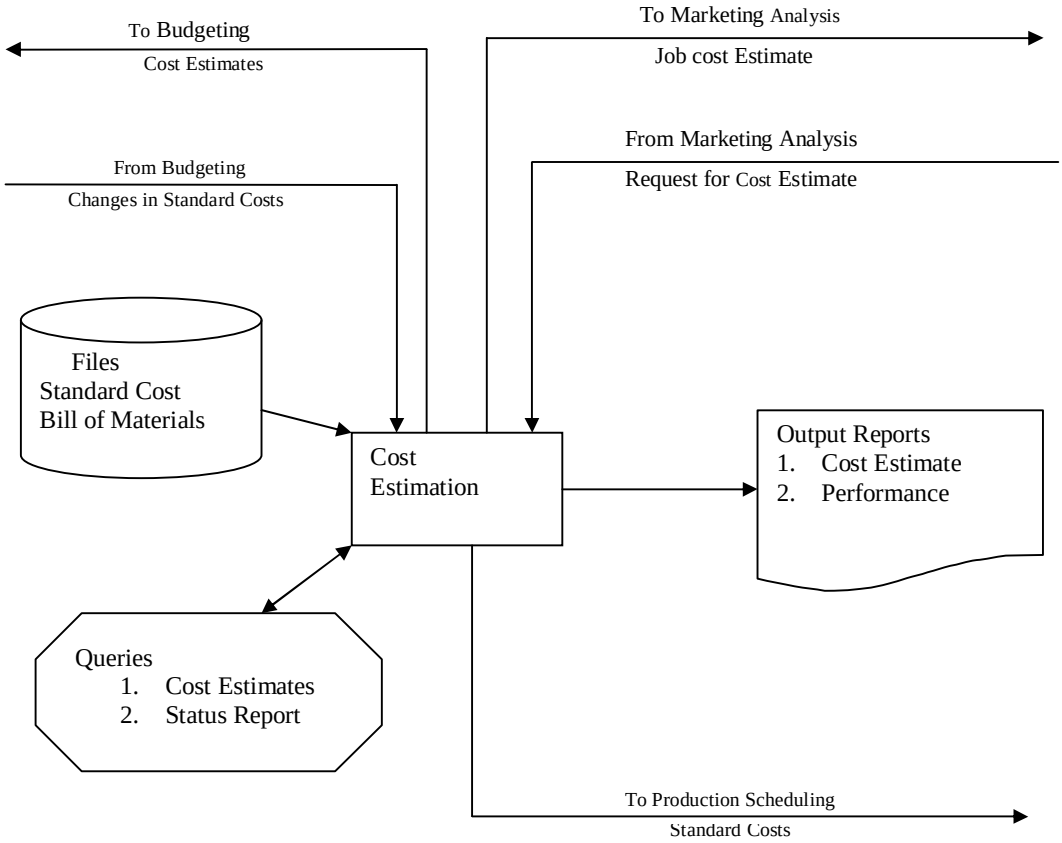
Reports

The work-in-process control system produces job cost, job status, and department performance reports periodically. A job cost report contains a detailed summary of the costs incurred to date, the budgeted cost, and estimated completion dates for each job is the system.

In departmental performance reports, costs are associated with department rather than jobs. These reports enable management to evaluate the performance of various departments.

COST ESTIMATION

A customer order is received by the firm after a customer has accepted an estimate of the cost of a job. The cost estimation system provides with manufacturing cost estimates based on inquiries received form potential customers. Cost estimates are a primary input when determining a price that will be quoted to a customer. When an order is received, the cost estimation system forwards the budgeted costs to the production scheduling system. Interfaces between the cost estimation system and other systems are shown in the figure. No function within the cost estimation system result in general ledger entries.



Cost Estimation System

System Interface

The cycle in the cost estimation system begins when the job specifications and a request for a cost estimate are received. Materials, machine time, and labour requirements for the job are then estimated and costed using standard costs. Overhead costs are also estimated, and the job cost estimate is then returned to the system. This estimate serves as the basis for the selling price that are quoted to the customer. When a customer's order is received, the standard costs for the job are transferred to the production scheduling system.

Files and inputs

The cost estimation system requires a standard cost file. Here, standard costs are maintained for each labour, material, and machine classification as well as for standard manufacturing operations. These costs are the basis for preparing manufacturing cost estimates. The standard costs are updated on the basis of information provided by the budgeting system.

The cost estimation system also maintains the bill of materials file, which contains a list of all materials, required to produce each product. The file also includes approved vendors for each material.

Reports

The cost estimation system can prepare manufacturing cost estimation reports for each job and performance measurement reports. The former are the primary output from the system. The performance measurement report shows how many cost estimation reports were processed and how many orders were received. The estimated and actual costs on orders received are compared for each cost classification. This enables over or under estimation to be identified.

PRODUCTION SCHEDULING

Production scheduling is the nerve centre of the production management system. It produces no general ledger journal entries, but it schedules production and monitors all physical flows. Given figure shows the information flow involving the production scheduling system.

System interfaces

The production scheduling system and various systems discussed earlier interact frequently. The sales order processing system authorizes production scheduling to start work on a job. Production scheduling then provides with estimated delivery dates and receives shipping reports from the finished goods inventory control system. Thus, all job scheduling information is kept in one system.
Within the production management system, the production scheduling and materials inventory control system interface frequently. Production scheduling informs materials inventory control of the items and quantities required to schedule production, and inventory control indicates the quantities available. Work-in-process control receives production authorization form the scheduling system. This authorization creates a new record for a job, and production costs can be charged to the job. At the same time, the work-in-process control system receives the standard cost for the job and provides status reports to the scheduling system. Cost estimation provides production scheduling with budgeted standard costs for all jobs production.

Files and Inputs

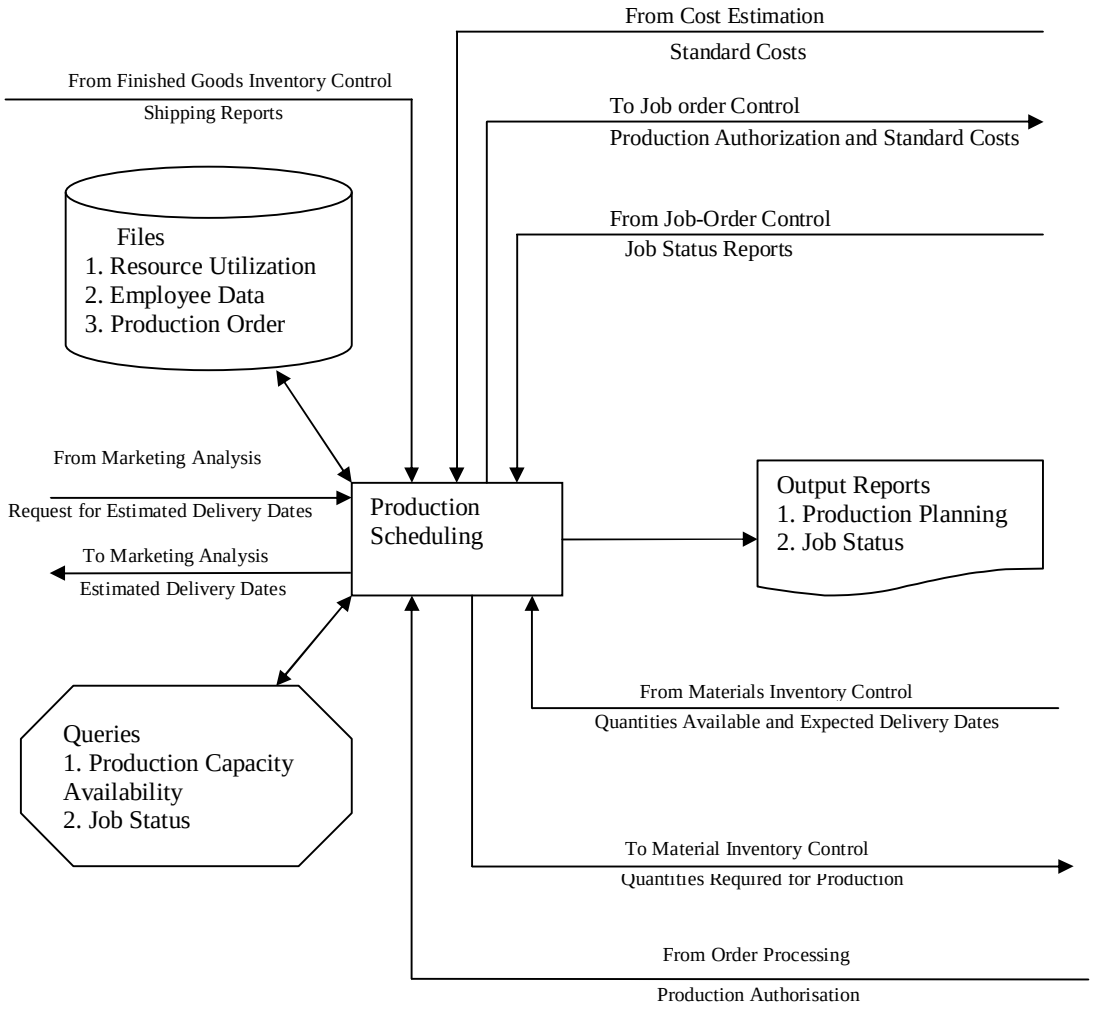
Three files are required in the production scheduling system. The resource utilization file contains a record for each machine and production process in the factory and maintains work schedules for them. The employee data file contains data concerning employee skills and scheduled work assignments. The production order file maintains completion dates and schedule information for each job.

Reports

The scheduling system produces periodic production planning reports. They indicate the available capacity and scheduled future utilization of labour and machinery. Such reports are useful to

management because they indicate where excess capacity exists for the planning period. Sales and pricing strategies can be considered to alleviate the situation. On the other hand, if frequent scheduling problems are encountered, then an adjustment in capacity may be necessary.

Job status reports concern the status of jobs in the production process. They compare scheduled and actual completion times in the production process. This report emphasizes scheduled times whereas the job order control report emphasizes costs.



Production Scheduling System

FINANCIAL ACCOUNTING

All organizations keep accounts. Accounting involves recording, classifying and summarizing transactions and events which are of financial nature. The results are analyzed. Financial accounting is mainly concerned with the preparation of profit and loss Statements and Balance Sheets. Modules for managing Accounts Receivables and Accounts Payable are often included in financial accounting packages.

Every transaction in a financial accounting system has a credit side and a debit side. The total debit amount in a transaction matches the total credit. One account head may be credited and another will be debited with the same amount. A transaction could involve multiple accounts being credited and debited while maintaining the total credit amount equal to the total debit amount.

Financial accounting is concerned with entering all transactions and keeping track of the balances of the various account heads. The summary of the balance and of the transactions is presented in the form of profit and loss statement and balance sheet. The reports are used to understand the financial operations of the organization.

Organizations are also concerned with the money owed by them to others (accounts payable) and amount of money which are owed to them (accounts receivable). Collection of money owed is usually a focus area for an organization and therefore an analysis of the accounts receivable is very important.

Financial accounting as an area is extremely amenable to computerization. All processing is well defined and numerical. Since accounts are subject to audit, existing manual systems are usually smooth and consequently the transition from manual systems to computer based systems is relatively smooth. The method of accounting is similar across companies, with a few minor differences. A large number of readymade software packages are available in the market.

To set up a financial accounting system, master data containing account heads (main as well as subsidiary accounts heads) along with a classification of accounts needs to be maintained.

The regular processing involves:

- entry of transactions
- printing of cash and bank books
- printing the general ledger
- producing the profit and loss statement and balance sheet
- producing other reports on accounts receivable and payable

Annual processing involves closing the year, producing year-end reports and initializing the account heads for a new year.

For processing, transactions form the regular input. The following transactions are typical in most financial accounting systems:

- sales invoices
- purchase bills
- payment vouchers (bank and cash)
- receipt vouchers (bank and cash)
- transfer of money between various bank accounts
- journal vouchers
- debit notes
- credit notes

while all transactions are essentially processed using the conventional double entry (debit and credit) system, different forms are used for different transactions in order to capture additional information (e.g., cheque number and date in a bank payment) and reference data.

Processing includes:

- Validation of the transactions-valid account heads, credit equal to debit, transaction date in valid range, etc.
- posting the transaction (credit and debit) under the correct account/sub account heads
- summarizing the accounts and transactions to produce the periodic profit and loss account and balance sheet
- printing details of accounts receivable (including age-wise analysis)
- printing details of accounts payable
- printing the day books and ledgers (records of transactions by date and type of transactions)
- facilitating reconciliation of accounting entries.

Annually, year-end activities require additional processing for incorporating the annual accounting entries and generating the Annual profit and loss statement and Annual Balance Sheet. After the annual reports are generated and found satisfactory, the accounts are initialized with the year opening balances for the next year's processing.

Outputs of financial accounting of financial accounting systems include:

- cash book
- bank book
- sales day book
- purchase day book
- general ledger
- subsidiary ledgers
- trial balance
- profit and loss statement (usually monthly/quarterly)
- balance sheet(usually month/quarterly)
- accounts receivable details
- customer statement of account
- age-wise accounts receivable
- account payable detail statement
- transaction details for given type of transaction, date range, account head, etc.,
- annual profit and loss statement
- annual balance sheet.

SHARE ACCOUNTING

Shares is an investment option used by many persons. A person may purchase shares either from the company (at the time of a public or a rights issue) or from the share market.

A share accounting system, needs to maintain an up to dated list of shareholders. For each shareholder, the main information held is the name and address, names of joint holders (if any) the number of shares held, and the identification of the certificates through which these shares are held.

When a person purchases shares from a share holder, 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 from the seller to the buyer.

Periodically, the company declares a dividend. Dividend warrants (cheques) need to be mailed on a particular day to the various shareholders who hold shares. Calculation of income tax to be deducted at source is also done before the printing and mailing dividend warrants.

Other facilities usually provided in share accounting system are:

- Bank mandate facility, where the shareholder's dividend warrant is sent to a bank account at the shareholders's request
- Splitting of share certificates, where a single certificate containing a large number of shares is replaced with a number of certificates containing a smaller number of shares
- Consolidation of shares, where many certificates belonging to a single shareholder are combined into one share certificate.
- Mailing annual reports and invitations to various meetings.

Main inputs to a share accounting system are:

- shareholding data from a fresh issue-this is usually supplied by the issue agency on electronic media
- share transfer request
- split request
- consolidation request
- request for bank mandate
- tax exemption forms
- request for duplicate certificates
- request for duplicate dividend warrants
- change in shareholder's address.

Processing involves:

- updating shareholders master file
- recording the transfer of shares
- handling splitting, consolidation and duplicate requests and printing new certificates
- calculation of dividend and income tax to be deducted.

Main outputs are:

- transferred share certificates
- new share certificates in case of consolidation, splitting and duplicates
- dividend warrants and counterfoils
- Statement of Tax deductions.

CHAPTER 12

ENTERPRISE RESOURCE PLANNING:REDESIGNING BUSINESS

INTRODUCTION

Enterprise Resource Planning (ERP) is the latest high-end solution, information technology has lent to business application. The ERP solutions seek to streamline and integrate operation processes and information flows in the company to synergise the resources of an organization namely men, material, money and machine through information.

As business needs are complex, the implementation of an ERP package need Chartered Accountants with functional skills for evaluation, Business Process Reengineering(BPR), mapping of business requirements, report designing, ensuring business controls, customization for specific requirements, documentation etc.

ERP-DEFINITION

An Enterprise resource planning system is a fully integrated business management system covering functional areas of an enterprise like logistics, Production, Finance, Accounting and Human Resources. It organizes and integrates operation processes and information flows to make optimum use of resources such as men, material, money and machine.

In simple words, Enterprise resource planning promises one database, one application, and one user interface for the entire enterprise, where once disparate systems rules manufacturing, distribution, finance and sales. Taking information from every function, it is a tool that assists employees and managers plan, monitor and control the entire business.

Evolution of ERP: In the ever-growing business environment, the following demands are placed on the industry:

- Aggressive cost control initiatives
- Need to analyse costs/revenues on a product or customer basis
- Flexibility to respond to changing business requirements
- More informed management decision making
- Changes in ways of doing business
- The difficulty in getting accurate data, timely information and proper interface of complex business functions, have been identified as the hurdles in the growth of any business.

One or the other applications and planning systems have been introduced into the business world for crossing these hurdles and achieving growth. They are:

1. Management Information System (MIS)
2. Integrated Information System (IIS)
3. Executive Information System (EIS)
4. Corporate Information System (CIS)
5. Enterprise Wide Systems (EWS)
6. Material Resource Planning (MRP)
7. Manufacturing Resource Planning (MRP II)
8. Money resource Planning (MRPIII)

The latest planning tool added to the above list is Enterprise Resource planning.

ENABLING TECHNOLOGIES: It is not possible to think of an ERP system without sophisticated information technology infrastructure. It is said that, the earlier ERP systems were built only to work with huge main frame computers. The new era of PC, advent of client server technology and scalable Relational Database Management Systems (RDBMS), all have contributed for the ease of

deployment of ERP systems. Most of the ERP systems exploit the power of Three Tier Client Server Architecture. In a client server environment, the server stores the data, maintaining its integrity and consistency and process the requests of the user from the client desktops. The load of data processing and application logic is divided between the server and the client.

It is assumed that the companies implementing ERP solutions have multiple locations of operation and control. Hence, the online data transfer has to be done across locations. To facilitate these transactions, the other important enabling technologies for ERP systems are Workflow, Work group, Group Ware, Electronic Data Interchange (EDI) Internet, Intranet, Data warehousing, etc.

ERP Characteristics:

Flexibility: An ERP system should be flexible to respond to the changing needs of an enterprise. The client server technologies enable ERP to run across various database back ends through Open Database Connectivity (ODBC).

Modular & Open: ERP system has to have open system architecture. This means that any module can be interfaced or detached whenever required without affecting the other modules. It should support multiple hardware platforms for the companies having heterogeneous collection of system. It must support some third party add-ons also.

Comprehensive: It should be able to support variety of organizational functions and must be suitable for a wide range of business organizations.

Beyond The Company: It should not be confined to the organizational boundaries. Rather support the on-line connectivity to the other business entities of the organization.

Best Business Practices: It must have a collection of the best business process applicable worldwide. An ERP package imposes its own logic on a company's strategy, culture and organization.

Features of ERP: Some of the major features of ERP and what ERP can do for the business system are:

- ERP provides multi-platform, multi-facility, multi-mode manufacturing, multi-currency, multi-lingual facilities.
- It supports strategic and business planning activities, operational planning and execution activities, creation of Materials and Resources. All these functions are effectively integrated for flow and update of information immediately upon entry of any information.
- Has end to end Supply Chain Management to optimize the overall Demand and Supply Data.
- ERP facilities company-wide Integrated Information System covering all functional areas like manufacturing, selling and distribution, payables, receivables, inventory accounts, human resources, purchases etc.
- ERP performs core activities and increases customer service, thereby augmenting the corporate image.
- ERP bridges the information gap across organizations.
- ERP provides complete integration of systems not only across departments but also across companies under the same management.
- ERP is the solution for better project management.
- ERP allows automatic introduction of the latest technologies like Electronic fund Transfer (EFT), Electronic Data Interchange (EDI), Internet, Intranet, Video conferencing, E-Commerce etc.
- ERP eliminates most business problems like material shortages, productivity enhancements, customer service, cash management, inventory problems, quality problems, prompt delivery etc.
- ERP provides business intelligence tools like Decision Support Systems (DSS), Executive Information System (EIS), Data Mining and easy working systems to enable better decisions.

Benefits of ERP:

The benefits accruing to any business enterprise by implementing an ERP package are unlimited. According to companies like Nike, DHL, Tektronix, Fujitsu, Milipore, and Sun Micro systems, the following are some of the benefits they achieved by implementing the ERP packages.

- Gives Accounts payable personnel increased control of invoicing and payment processing and thereby boosting their productivity and eliminating their reliance on computer personnel for these operations.
- Reducing paper documents by providing on-line formats for quickly entering and retrieving information.
- Improves timeliness of information by permitting posting daily instead of monthly.
- Greater accuracy of information with detailed content, better presentation, satisfactory for the auditors.
- Improved cost control.
- Faster response and follow-up on customers.
- More efficient cash collection, say, material reduction in delay in payments by customers.
- Better monitoring and quicker resolution of queries.
- Enables quick response to change in business operations and market conditions.
- Helps to achieve competitive advantage by improving its business process.
- Improves supply-demand linkage with remote locations and branches in different countries.
- Provides a unified customer database usable by all applications.
- Improves international operations by supporting a variety of tax structures, invoicing schemes, multiple currencies, multiple period accounting and languages.
- Improves information access and management throughout the enterprise.
- Provides solution for problems like y2k and single monetary Unit (SMU) or Euro Currency.

BUSINESS PROCESS REENGINERING (BPR)

ERP is a result of a modern Enterprise's concept of how the Information System is to be configured to the challenging environments of new business opportunities. However merely putting in place an information system is not enough. Every company that intends to implement ERP has to reengineer its processes in one form or the other. This process is known as Business Process Reengineering (BPR).

What is BPR?

The most accepted and formal definition for BRP, given by Hammer and Chaphy is reproduced here: "BPR is the fundamental rethinking and radical redesign of processes to achieve dramatic improvement, in critical, contemporary measures of performance such as cost, quality, service and speed".

This has a few important key words, which need clear understanding. Here dramatic achievement means to achieve 80% or 90% reduction (in say, delivery time, work in progress or rejection rate) and not just 5%, 10% reduction. This is possible only by making major improvements and breakthroughs, and not small incremental changes.

Radical redesign means BPR is reinventing and not enhancing or improving. In a nutshell, a "clean site approach" or BPR says that "what ever we were doing in the past is all wrong". Fundamental rethinking means asking the question "why do we do what we do", thereby eliminating business process altogether if it does not add any value to the customer. There is no point in simplifying or automating a business process which does not add any value to the customer. A class example is that of asking for an invoice from the supplier for payment when the company has already received and accepted a particular quantity of materials physically and at an agreed price. Receiving, processing, and filing of invoices add no value to customer and makes only the supplier unhappy for delayed payments. Thus, BPR aims at major transformation of the business processes to achieve Dramatic improvement. Here, the business objectives of the Enterprise (e.g., profits, customer-satisfaction

through optimal cost, quality, deliveries etc) are achieved by "transformation" of the business processes which may, or may not, require the use of Information Technology (IT).

ERP IMPLEMENTATION.

ERP implementation is a special event in an organization. It brings together in one platform, different business functions, different personalities, procedures, ideologies and philosophies with an aim to pool knowledge base to effectively integrate and bring worthwhile and beneficial changes throughout the organization. Implementation of ERP is a risky effort since it involves considerable amount of time, efforts and valuable resources. Even with all these, the success of an implementation is not guaranteed.

The success of an implementation mainly depends on how closely the implementation consultants, users and vendors work together to achieve the overall objectives of the organization. The implementation consultant has to understand the needs of the users, understand the prevailing business realties and design the business solutions keeping in mind all these factors. It is the users who will be driving the implementation and therefore their active involvement at all stages of implementation is vital for the overall success of implementation.

The roles and responsibilities of the employees have to be clearly identified, understood and configured in the system. The employees will have to accept new process and procedures laid down in the ERP system. At the same time these processes and procedures have to be simple and user friendly.

ERP implementation Methodology

Several steps are involved in the implementation of a typical ERP package. These are:

1. Identifying the needs for implementing an ERP package.
2. Evaluating the 'As Is' situation of the business i.e., to understood the strength and weakness prevailing under the existing circumstances.
3. Deciding the 'Would be' situation for the business i.e., the changes expected after the implementation of ERP.
4. Reengineering the Business Process to achieve the desired results in the existing processes.
5. Evaluating the various available ERP packages to assess suitability.
6. Finalising of the most suitable ERP package for implementation.
7. Installing the required hardware and networks for the selected ERP package.
8. Finalising the Implementation consultants who will assist in implementation.
9. Implementing the ERP package.

Let us examine these steps in detail:

1. **Identifying the Needs:** Some of the basic questions, which are to be answered, are
   - Why should an ERP package be implemented?
   - Will it improve profitability?
   - Can the delivery time of products be reduced?
   - How does it improve customer satisfaction in terms of quality, cost, delivery time and service?
   - Will it help to reduce cost of products?
   - How can it help to increase business turnover and at the same time reduce manpower?
   - Will it be possible to reengineer the business processes?

   Other requirements to satisfy the information management are
   - Need for quick flow of information between Business partners.
   - Effective MIS for quick decision making
   - Elimination of manual working.
   - High level of integration between various business functions.

2. **Evaluating the "AS IS" situation of the business:** To understand the present situation of the business, the various functions should first be listed. The processes used to achieve business transactions should be listed in detail. The details of business process can be obtained by mapping the process to the functions.

- Total time taken by the business processes.
- Number of decision points existing in the present scenario.
- Number of Departments/Locations of business processes.
- The flow of information and its routing.
- The number of reporting points currently available.

3. **Deciding the desired 'Would Be' situation:** The concept of 'Benchmarking' is used to see that processes achieved are the best in industry. Benchmarking is done on various factors like cost, quality, service etc. This concept enables to optimise the processes to gain overall benefits.
4. **Reengineering the business process:-** Reengineering of business processes is done to
   - Reduce the business process cycle time.
   - To reduce the number of decision points to a minimum.
   - Streamlining the flow of information and eliminating the unwanted flow of information.

5. **Evaluation of various ERP packages:**
Evaluation of ERP packages are done based on the following criteria:

Flexibility: It should enable organizations to respond quickly by leveraging changes to their advantage, letting them concentrate on strategically expanding to address new products and markets.

Comprehensive: It should be applicable across all sizes, functions and industries. It should have in-depth features in accounting and controlling, production and materials management, quality management and plant maintenance, sales and distribution, human resources management, plant maintenance, and project management. It should also have information and early warning systems for each function and enterprise-wide business intelligence system for informed decision making at all levels. It should be open and modular.

It should embrace an architecture that supports components or modules, which can be used individually, expandable in stages to meet the specific requirements of the business, including industry specific functionality. It should be technology independent and mesh smoothly with in-house/third-party applications, solutions and services including the Web.

Integrated: It should overcome the limitations of traditional hierarchical and function oriented structures. Functions like sales and materials planning, production planning, warehouse management, financial accounting, and human resources management should be integrated into a workflow of business events and processes across departments and functional areas, enabling knowledge workers to receive the right information and documents at the right time at desktops across organizational and geographical boundaries.

Beyond the company: It should support and enable inter-enterprise business processes with customers, suppliers, banks, government and business partners and create complete logistical chains covering the entire route from supply to delivery, across multiple geographies, currencies and country specific business rules.

Best business practices: The software should enable integration of all business operation in all overall system for planning, controlling and monitoring and offer a choice of multiple ready-made business processes including best business practices that reflect the experiences, suggestions and requirements of leading companies across industries. In other words, it should intrinsically have a rich wealth of business and organizational knowledge base.

New technologies: It should incorporate cutting-edge and future-proof technologies such as object orientation into product development and ensure inter-operability with the Internet and other emerging technologies.

It should be Y2K and Euro complain, group up.
Other factors to be considered are:

- Global presence of package.
- Local presence.
- Market Targeted by the package.
- Price of the package.
- Obsolescence of package.
- Ease of implementation of package.
- Cost of implementation.
- Post-implementation support availability.

6. **Finalization of the ERP package:** Finalization of the ERP package can be done by making a comparison of critical factors through a matrix analysis.

7. **Installation of Hardware and Networks:** This work is carried out in a phased manner depending on the schedule of implementation and need of the hardware components.

8. **Finalizing the Implementation Consultants:** The factors of selection for consultants are:

- Skill set
- Industry specific experience
- Cost of hiring the consultant.

9. **Implementation of ERP package:** The general steps involved in the implementation are:

- Formation of team.
- Preparation of plan.
- Mapping of Business Processes to package.
- Gap Analysis i.e., deviation of existing processes from standard processes.
- Customization.
- Development of user-specific reports and transactions.
- Uploading of Data from existing system.
- Test runs.
- User Training.
- Parallel run.
- Concurrence from user.
- Migration to the new system.
- User documentation support.
- System monitoring and fine-tuning.

Implementation Guidelines for ERP:
There are certain general guidelines, which are to be followed before starting the implementation of an ERP package.

1. Understanding the corporate needs and culture of the organization and then adopt the implement technique to match these factors.
2. Doing a business process redesign exercise prior to starting the implementation.
3. Establishing a good communication network across the organization.
4. Providing a strong and effective leadership so that people down the line are well motivated.
5. Finding an efficient and capable project manager.
6. Creating a balanced team of implementation consultants who can work together as a team.
7. Selecting a good implementation methodology with minimum customization.

8. Training end users.
9. Adapting the new system and making the required changes in the working environment to make effective use of the system in future.

POST–IMPLEMENTATION

To start at the beginning, many post-implementation problems can be traced to wrong expectations and fears. The expectations and fears that corporate management has from and ERP have been greatly published. Of course, some of the blame for this is on the ERP vendors and their pre-implementation sales hype.

A few of the popular expectations are:

- an improvement in processes.
- Increased productivity on all fronts.
- Total automation and disbanding of all manual processes.
- Improvement of all key performance indicators.
- Elimination of all manual record keeping.
- Real time information systems available to concerned people on a need basis.
- Total Integration of all operations.

ERP implementation also cause a host of fears. Some of them are:

- Job redundancy.
- Loss of importance as information is no longer an individual prerogative.
- Change in job profile.
- An organizational fear of loss of proper control and authorization.
- Increased stress caused by greater transparency.
- Individual fear of loss of authority.

Balancing the expectations and fears is a very necessary part of the implementation process.
Now comes the reality part. A few of the realities that any organization must keep in mind are:

- Changing the organization involves three leverl-strategic, business process and change, and consequential organization change.
- Changing the organization requires a mindset change. Without a willingness to change, it would be a classic case of an old organization plus new technology leading to an expensive old organization.
- In most companies in India, many process related key performance indicators have not been measured till now-either because the company did not feel it necessary or lacked the tools to do so. Measuring such indicators brings in new culture.
- The genetic nature of the ERP packages is such that there would be processes peculiar to some sectors and organizations, which may have to be kept out of the process.
- Some of the processes are better done manually.
- Finally, a successful ERP implementation is not the end of the road as far as change is concerned, and continuous improvements are required to reap the benefits. The expectations, fears and reality can most obviously be balanced during the process of implementation itself.

SAMPLE LIST OF ERP VENDORS

This is only a sample listing of ERP Vendors. It may not be comprehensive.

Baan (The Baan Company) : In 1994, a Boeing order launched Baan into the global ERP vendor league. Baan has held and built on this position with other major orders and a strategy for simultaneously addressing manufactures from the largest global player to the smallest ERP user. Baan has a sound technology base and a broad functional scope. It offers credible tools for business process analysis linked to implementation of its software, and is launching work flow capabilities to build on this.

Business Planning and Control System (BPCS): BPCS remains the market-leading manufacturing ERP solution in terms of sites. It only targets manufacturing companies. It offers good functionality for process, discrete manufacturing, but not for project management. It lags in the areas of process-oriented implementation tools and workflow. It has made mistakes, its developments have not run to schedule and it has incurred enormous losses.

Mapics XA (Marcam Corporation): Mapics has been around for a long time. Mapics is a suite of 40 modules with 'good enough' functionality. Many users report that Mapics now offers more functionality than they need. It offers robustness, easy implementation and reasonable value for money.

MFG/Pro (QAD): QAD's strength is in repetitive manufacturing. Originally designed to meet the MRP II criteria published by Oliver Wight. MFG/Pro's reputation includes reliable manufacturing functionality and straightforward implementations.

Oracle Applications (Oracle): Oracle's Manufacturing Applications will tempt IT departments, with its vision of Internet-enabled, network-centric computing. As a one stop shop, it offers the database, tools, implementation, applications and Unix operating systems running on a wide choice of hardware. Oracle has invested heavily to enhance functionality but production managers should still check that it delivers all the functionality they want.

Prism (Marcam Corporation): Prism is a specialist process manufacturing solution for the AS/400. Its production model, which is akin to a flowchart, handles process industry problems elegantly. Although out dated, it does the job.

R/3 (SAP): In five years, R/3 is the market leader in new sales. Its philosophy of matching business processes to modules is excellent. It offers a wide range of functions and its major shortcomings are yet to be identified. However, it remains complex, because it offers much; few people know how to get the best from it. R/3 will be around for a long time.

System 21 (JBA): JBA develops and implements System 21. Its software license revenues are small compared to those of other major ERP vendors. Nevertheless, it is a world player. It does not offer leading-edge technology, but does offer a rugged, reliable manufacturing solution.

CASE STUDY

Videocon Group

Getting into the groove: Consolidation of information flowing in from a multi-branch factory and multi operation was the main driver behind the Videocon Group's decision implement an Enterprise Resource Planning (ERP) package.

"For a multi-manufacturing, multi-branch company like ours, the one major essential was centralized and consolidated information that is available in a uniform manner across various levels in the orgnizations," says Pradip Kumar N Dhoot, President, Videocon International.

"The factories were already working on legacy systems using an Intranet and collating information. But each factory and branch would use different software, varied platforms, which did not speak to each other. This not only resulted in huge inflow of data which could not be consolidated for analysis but also duplication of data", Videocon is a $ 1-billion company. Even one per cent change in any data entry or analysis translates into millions and can sometimes wipe out the profits of the organization. So they needed a system that would help them to be responsive and act fast.

Further, at some stage they wanted to share a common platform with their dealers so that they could access the company servers and database, get updates on issues relating specifically to them as well as the company on the whole.

The mandate: It was in 1998 that Videocon began evaluating ERP packages and roped in the pune-based Ygyan Consulting to help select and implement an appropriate package. In August 1998, based on Ygyan's recommendations, SAP's ERP package was finally selected.

The issues that needed to be addressed included:

- Better inventory management and control.
- Improved financial reporting and control.
- Automation of certain tasks that were performed manually to increase productivity.
- Improved production planning.
- Better information on stocks at various locations.
- Using an integrated system as opposed to disparate systems at different locations thereby eliminating errors of duplicate entries.
- More accurate costing of products.
- Better credit control.
- Improved cash flow planning.
- Automatic quality-control and tracking.
- Better after-sales-service.
- Better information and reporting to top management.

Going about the implementation: For the implementation, Ygyan first tied up with Siemens Information systems Ltd. (SISL) for a pilot project at the first site—Videocon Appliances Ltd. The modules implemented were finance and Control, Materials Management, Sales and Distribution, production Planning and Quality Management.

Videocon International was next in line. The scope of the project included all modules mentioned above in addition to a Plant Maintenance module. The implementation was divided into two phases where the four factories went first, followed by marketing operations across the country. The factories are located in Aurangabad, Bharuch, Gandhinagar and Bhalgaon.

Factories (Parent units) went live first, within a year, and have been live for the past two years. They decide to go with the factories first because they are situated close to each other, compared to the branches, which are scattered across the country.

During the implementation, connectivity was a problem. So Ygyan suggested a mix of leased line, ISDN, VSATs and Internet connectivity to optimise the costs while ensuring enough speed for users connecting from remote locations.

The entire process took eight months, right from drawing up the blue prints, consulting, customising and training core teams. The Group almost invested in excess of Rs. 25 crore for the implementation, including the ERP package, hardware, connectivity etc., excluding the maintenance charges.

The biggest question that they had to ask themselves was whether or not they wanted transparency.. that's the first thing that comes to light once ERP is in place since ERP involves a top downward approach—from a sales person to the top management, everybody is accountable.

The most important issue in the implementation of any technology is the attitude of the employees, it has to change—from working for oneself to working as a whole for the organization. Employees too had their own fears and apprehensions about the system. A strong fear was that of retrenchment as a result of the implementation. However, the company held adequate training workshops at central and state level. In the factories, various processes were documented using print and audio/video to facilitate training on new employees".

On the whole, employee reaction was positive as people were already using computers and an Intranet to send information. The initial apprehension fell through once people started using the system.

Lessons to learn: There were a few areas in which they did face problems with the package, as it does not have modules specific to Indian requirements such as taxes, Letter of Credits (LCs), import clearance and product evolution. In fact, a product evolution module is very essential for a consumer durable company, as it is needed to develop products according to market feedback. For a durable company, a new development would cost crores and be spread across 18 months or so. A product evolution module can be of great help in this scenario, the company management feels.

Looking ahead: It was reported in October, 2001, that Ygyan is now in the process of rolling out SAP in all other group companies, one at a time. The company managers are also working with the in other IT initiatives, including e-business and Internet-based customer relationship management systems.

The next step will be to see how system can be extended to include the partners and dealers. But that will start only after six-eight months once the employee get completely comfortable with the system. CRM is another area that the company is interested in.

CASE STUDY/TELCOM

Company: Air Touch Cellular: Industry: Telecom : Solution Area: Financials

Air Touch Cellular is a subsidiary of Air Touch Communications, a global wireless communications company serving 6.7 million customers worldwide in the areas of cellular, paging, personal communications services (PCS) and Globalstar satellite system markets.

Problem: Air Touch's Financial analysts, located in different functional groups in five geographic regions, were missing access to the same data, as well as timely access to information. Dated budget and actual numbers for each business unit resided in seven different systems, separating critical components of the Profit and Loss A/c and inhibiting analysts' ability to assess results. To further complicate matters, analysts in the field could not go to one universal place to retrieve the data themselves-they relied on the home office to deliver it. The company wanted to set some critical financial objectives to help it remain competitive and increase market share.

Air Touch chose Oracle Corporation's online analytical processing (OLAP) tools to better control costs, analyze performance, evaluate opportunities, and formulate future direction. And to improve the basis for making decisions quickly and accurately with real-time, consistent data; to improve cost control, and to simplify and shorten the budgeting process.

Implementation: AirTouch Cellular looked at two other vendors before choosing Oracle, but neither could provide users with the hands-on ability to consolidate budgets, include actuals in the process, or do what-if scenarios online. Air Touch Cellular's parent company also had a proven, successful track record with other Oracle applications and a corporate initiative to make Oracle the vendor of choice.

Oracle provided on-site expertise in the product, the concept, and the business to create a user-friendly system. The project came in on time and within budget, with very few post implementation issues. Completing the entire implementation in eight months was quite a feat, given the many changes that occurred in that time frame, according to the company.

Not only did the company convert to a new system, it completely overhauled the budget process and the P&L reporting format - among departmental and company reorganizations.

Benefits: It resulted into more than $8 million in hard and soft dollar savings. Also, it reduced the length of the budgeting cycle and the number of people involve in the process, keeping the company financially competitive in a growing market. The system now provides online, real-time access to information.

Now, analysis can individually access the same data warehouse for current, real-time information for their analysis. This means the vice presidents from each business unit in the division now have the data they need-budget or actual-on a timely basis. Thus enabling business units to make better, faster business decisions based on more accurate information. Their increased understanding of the data help them run their slices of the business more effectively, because they can now make real-time, online decisions that help them stay on budget or shift business direction.

CHAPTER 13

CONTROLS IN EDP SET-UP: GENERAL CONTROLS

TYPES OF CONTROLS IN A COMPUTER-BASED SYSTEM

Computer based information system internal controls are divided into following broad categories:

1. **General controls:** These controls apply to a wide range of exposures that systematically threaten the integrity of all applications processed within the computer Based Information system (CBIS) environment. General controls can be further subdivided under following headings:

    a. Operating system controls,
    b. Data management controls,
    c. Organizational structure controls,
    d. Systems development controls,
    e. Systems maintenance controls,
    f. Computer centre security controls,
    g. Internet and Intranet control,
    h. Personal computer controls.

2. **Application Controls:** These controls are focused on exposures associated with specific systems, such as payroll, accounts receivables, and so on.

GENERAL CONTROLS: OPERATING SYSTEM CONTROLS

The Operating System is the computer's control program. It allows users and their applications to share and access common computer resources, such as processors, main memory, databases, and printers.

If operating system integrity is compromised, controls within individual accounting applications may also be neutralized.

The operating system performs three main tasks. First, it translates high-level languages, such as COBOL, FORTRAN, BASIC and SQL into the machine-level language that the computer can execute.

Second, the operating system allocates computer resources to users, workgroups, and applications. This includes assigning memory work space (partitions) to applications and authorizing access to terminals, telecommunications links, databases, and printers.

Third, the operating system manages the tasks of job scheduling and multiprogramming.

To perform these tasks consistently and reliably, the operating systems must achieve five fundamental control objectives.

1. The operating system must protect itself from users. User applications must not be able to gain control of, or damage in any way, the operating system, thus causing it to cease running or destroy data.
2. The operating system must protect users from each other. One user must not be able to access, destroy, or corrupt the data or programs of another user.
3. The operating system must protect users from themselves. A user's application may consist of several modules stored in separate memory locations, each with its own data. One module must not be allowed to destroy or corrupt another module.
4. The operating system must be protected from itself. The operating system is also made up of individual modules. No module should allowed to destroy or corrupt another module.

5. The operating system must be protected from its environment. In the event of a power failure or other disaster, the operating system should be able to achieve a controlled termination of activities from which it can later recover.

Operating System Security: Operating system security involves policy, procedures, and controls that determine who can access the operating system, which resources (files, programs, printers) they can access and what actions they can take. The following security components are found in secure operating systems.

Log-On Procedure: A formal log-on procedure is the operating system's first line of defense against unauthorized access. When the user initiates the process, he or she is presented with a dialog box requesting the user's ID and password. The system compares the ID and password to a database of valid users. If the system finds a match, then the log-on attempt is authenticated. If, however, the password or ID is entered incorrectly, the log-on attempt fails and a message is returned to the user. The message should not reveal whether the password or the ID caused the failure. The system should allow the user to reenter the log-on information. After a specified number of attempts (usually not more than five), the system should lock out the user from the system.

Access token: If the log-on attempt is successful, the operating system creates an access token that contains key information about the users, including user ID, password, user group, and privileges granted to the user. The information in the access token is used to approve all actions attempted by the user during the session.

Access Control List: Access to system resources such as directories, files, programs, and printers are controlled by an access control list assigned to each resource. These lists contain information that defines the access privileges for all valid users of the resource. When a user attempts to access a resource, the system compares his or her ID and privileges contained in the access token with those contained in the access control list. If there is a match, the user is granted access.

Discretionary Access Control: The system administrator usually determines who is granted access to specific resources and maintains the access control list. In distributed system, however, resources may be controlled (owned) by end users. Resource owners in this setting may be granted discretionary access control, which allows them to grant access privileges to other users. For example, the controller, who is the owner of the general ledger, grants read-only privileges to a manager in the budgeting department. The accounts payable manager, however, is granted both read and write permission to the ledger. Any attempt by the budgeting manager to add, delete, or change the general ledger will be denied. The use of discretionary access control needs to be closely supervised to prevent security breaches due to its liberal use.

Threats to Operating System Integrity: Operating system control objectives are sometimes not achieved because of flaws in the operating system that are exploited either accidentally or intentionally.

Accidental threats include hardware failures that cause the operating system to crash. Operating system failures are also caused by errors in user application programs that the operating system cannot interpret. Accidental system failures may cause whole segments of memory to be "dumped" to disks and printers, resulting in the unintentional disclosure of confidential information.

Intentional threats to the operating system are most commonly attempts to illegally access data or violate user privacy for financial gain. However, a growing form of threat is from destructive programs from which there is no apparent gain.

Controlling Access Privileges: User access privileges are assigned to individuals and to entire workgroups authorized to use the system. Privileges determine which directories, files, applications, and other resources an individual or group may access.

Overall system security is influenced by the way access privileges are assigned. Privileges should therefore, be carefully administered and closely monitored for compliance with organizational policy and principles of internal control.

Password Control: A password is a secret code entered by the user to gain access to systems, applications, data files, or a network server. If the user cannot provide the correct password, the operating system should deny access.

Reusable Passwords: The most common method of password control is the reusable password. The user defines the password to the system once and then reuses it to gain future access. Most operating systems set only basic standards for password acceptability. The quality of the security provided by a reusable password depends on the quality of the password itself. If the password pertains to something personal about the user, such as child's name, pet's name, birth date, or hair colour, it can be deduced by a computer criminal.

To improve access control, management should discourage the use of "weak" passwords. Inexpensive software is available that automatically scans password files and notifies the security administrator when weak passwords are detected, thus assuring that only "smart" passwords are used on the system. An alternative to the standard reusable password is the one-time password.

One-time Passwords: The one-time password was designed to overcome the problems just discussed. Under this approach, the user's password changes continuously. To access the operating system, the user must provide both a secret reusable personal identification number (PIN) and the current one-time-only password for that point in time. The problem, of course, is how to advise the valid user of the current password.

Controlling Against Virus and other Destructive Programs: Destructive programs such as viruses are responsible for huge amount of corporate losses annually. The losses are measured in terms of data corruption and destruction, degraded computer performance, hardware destruction, violations of privacy, and the personnel time devoted for repairing the damage. We have discussed below some of the more common type of destructive programs.

Virus: A virus is a program (usually destructive) that attaches itself to a legitimate program to penetrate the operating system. The virus destroys application programs, data files, and operating systems in a number of ways. One common technique is for the virus to simply replicate itself over and over within the main memory, thus destroying whatever data or programs are resident. One of the most insidious aspects of a virus is its ability to spread throughout the system and to other systems before perpetrating its destructive acts. Typically, a virus will have a built-in counter that will inhibit its destructive role until the virus has copied itself a specified number of times to other programs and systems. The virus thus grows geometrically, which makes tracing its origin extremely difficult.

Virus programs usually attach themselves to the following types of files:
1. An.EXE or .COM program file
2. The.OVL (overlay) program file
3. The boot sector of a disk
4. A device driver program.

When a virus-infected program is executed, the virus searches the system for uninfected programs and copies itself into these programs. The virus in this way thus spreads to the applications of other users or to the operating system itself.

Worm: The term worm is used interchangeably with virus. A worm is a software program that "burrows" into the computer's memory and replicates itself into areas of idle memory. The worm systematically occupies idle memory until the memory is exhausted and the system fails. Worms differ from viruses in that the replicated worm modules remain in contact with the original worm that controls their growth. The replicated virus modules, on the other hand, grow independently of the initial virus.

Logic Bomb: A logic bomb is a destructive program, such as a virus, that is triggered by some predetermined event. Quite often a date (such as Friday the 13th, April Fool's day, or birthday) will be the logic bomb's trigger. The famous Michelangelo virus (triggered by his birth date) is an example of a logic bomb.

Back Door: A back door (also called a trap door) is a software program that allows unauthorized access to a system without going through the normal (front door) log-on procedure. Programmers who want to provide themselves with unrestricted access to the program that they are developing for users may create a log-on procedure that will accept both the user's private password and their own secret password, thus creating a back door to the system. The purpose of the back door may be to provide easy access to perform program maintenance, or it may be to perpetrate a fraud or insert a virus into the system.

Trojan Horse: A Trojan horse is a program whose purpose is to capture Ids and passwords from unsuspecting users. The program is designed to mimic the normal log-on procedures of the operating system. When the user enters his or her ID and password, the Trojan horse stores a copy of them in a secret file. At some later date, the author of the Trojan horse uses these ids and passwords to access the system and masquerade as an authorized user.

Threats from destructive programs can be substantially reduced through a combination of technology controls and administrative procedures. The following examples are relevant to most operating systems.

- Purchase software only from reputable vendors and accept only those products that are in their original, factory-sealed packages.
- Examine all upgrades to vendor software for viruses before they are implemented.
- Establish an educational program to raise user awareness regarding threats from viruses and malicious programs.
- Install all new applications on a stand-alone computer and thoroughly test them with antiviral software prior to implementing them on the mainframe or LAN server.
- Routinely make backup copies of key files stored on mainframes, servers, and workstations.
- Use antiviral software (also called vaccines) to examine application and operating system program for the presence of a virus and remove it from the affected program. Antiviral programs are used to safeguard mainframes, network servers, and personal computers. Most antiviral programs run in the background on the host computer and automatically test all files that are uploaded to the host. However, the software works only on known viruses. If a virus has been modified slightly, there is no guarantee that the vaccine will work. It is therefore important to maintain the current version of the vaccine.

Controlling Audit Trails: Audit trails are logs that can be designed to record activity at the system, application, and user level. When properly implemented, audit trails provide an important detective control to help accomplish security policy objectives. Many operating systems allow management to select the level of auditing to be provided by the system. This determines which events will be recorded in the log. An effective audit policy will capture all significant events without cluttering the log with trivial activity.

Audit Trail Objectives: Audit trails can be used to support security objectives in three ways:

1. Detecting unauthorized access to the system.
2. Facilitating the reconstruction of events, and
3. Promoting personal accountability.

1. *Detecting Unauthorized Access:* Detecting unauthorized access can occur in real time or after the fact. The primary objective of real-time detection is to protect the system from outsiders who are attempting to breach system controls. A real-time audit trail can also be used to report on changes in system performance that may indicate spread of virus or worm. After-the-fact detection logs can be stored electronically and reviewed periodically or as needed. When properly designed, they can be used to determine if unauthorized access was accomplished, or attempted and failed.
2. *Reconstructing Events:* Audit analysis can be used to reconstruct the steps that led to events such as system failures, security violations by individuals, or application processing errors. Knowledge of the conditions that existed at the time of a system failure can be used to assign responsibility and to avoid similar situations in the future. Audit trail analysis also plays an important role in accounting control. For example, by maintaining a record of all changes to account balances, the audit trail can be used to reconstruct accounting data files that were corrupted by a system failure.
3. *Personal Accountability:* Audit trails can be used to monitor user activity at the lowest level of detail. This capability is a preventive control that can be used to influence behavior. Individual are likely to violate an organization's security policy if they know that their actions are recorded in an audit log.

Implementing an Audit Trail: The information contained in audit logs is useful to accountants in measuring the potential damage and financial loss associate with application errors, abuse of authority, or unauthorized access by outside intruders. Logs also provide valuable evidence or assessing both the adequacies of controls in place and the need for additional controls. Audit logs, however, can generate data in overwhelming detail. Important information can easily get lost among the superfluous detail of daily operation. Thus, poorly designed logs can actually be dysfunctional.

GENERAL CONTROLS: DATA MANAGEMENT CONTROLS

Controls over data management fall into two general categories: access controls and backup controls.

- Access controls are designed to prevent unauthorized individuals from viewing, retrieving, corrupting, or destroying the entity's data.
- Backup controls ensure that in the event of data loss due to unauthorized access, equipment failure, or physical disaster, the organization can recover its files and databases.

Access Controls: Users of flat file systems maintain exclusive ownership of their data. In spite of the data integration problems associated with the model, it creates an environment in which unauthorized access to data can be effectively controlled. When not in use by the owner, a flat file is closed to other users and may be taken off-line and physically secured in the data library. In contrast, the need to integrate and share data in the database environment means that databases must remain on-line and open to all potential users.

Several database control features are reviewed below.

a. User View: The user view or sub schema is a subset of the total database that defines the user's data domain and provides access to the database. Though the DBA has primary responsibility for user view design, he works closely with users and systems designers in this task. Access privileges to the data, as defined in their views, should be commensurate with the users' legitimate needs.

Although user views can restrict user access to a limited set of data, they do not define task privileges such as read, delete, or write. Often, several users may share a single user view but have different authority levels. Effective access control requires additional security measures.

b. *Database Authorization Table:* The database authorization table contains rules that limit those actions a user can take. This technique is similar to the access control list used in the operating system. Each user is granted certain privileges that are coded in the authority table, which is used to verify the user's action requests. Each row in the authority table indicates the level of action (read, insert, modify, or delete) that individuals can take based on their entering the correct password.

Dept	Accounts Receivable			Billings	
User	Jai	Suresh	Aman	Mohan	Vimal
Password	Bugs	Dog	Katie	Lucky	Star
Authority:					
Read	Y	Y	Y	Y	Y
Insert	Y	N	Y	Y	N
Modify	Y	N	N	Y	N
Delete	Y	N	N	N	N

c. User-Defined Procedures: A user defined procedure allows the user to create a personal security program or routine to provide more positive user identification than a single password can. For example, in addition to a password, the security procedure asks a series of personal questions (such as the user's mother's maiden name), which only the legitimate user is likely to know.

d. *Data Encryption:* Many database systems use encryption procedures to protect highly sensitive data, such as product formulae, personnel pay rates, password files, and certain financial data. Data encryption uses an algorithm to scramble selected data, thus making it unreadable to an intruder "browsing" the database. In addition to protecting stored data, encryption is used for protecting data that are transmitted across networks.

e. *Biometric Devices:* The ultimate in user authentication procedures is the use of biometric devices, which measure various personal characteristics, such as fingerprints, voice prints, retina prints, or signature characteristics. These user characteristics are digitized and stored permanently in a database security file or on an identification card that the user carries. When an individual attempts to access the database, a special scanning device captures his or her biometric characteristics, which is compared with the profile data stored internally or on the ID card, if the data do not match, access is denied. Biometric technology is currently being used to secure ATM cards and credit cards.

Back-up Controls: Data can be corrupted and destroyed by malicious acts from external hackers, disgruntled employees, disk failure, program errors, fires, floods, and earthquakes. To recover from such disasters, organizations must implement policies, procedures and techniques that systematically and routinely provide backup copies of critical files.

Often, the originals are stored at site that is physically distant from the actual site, and where duplicate copies are used for processing. The backup copies must be kept in a place which is not susceptible to the same hazards as the originals.

1. *The file security:* The techniques employed for reconstruction of master files on magnetic disks and tapes, in the event of their loss/destruction are outlined below:

a. Magnetic Disk: In the case of magnetic disk, file security is carried out in the following manner:

Contents of master file on magnetic disk are periodically copied or dumped on magnetic tape backup file and stored at another location. A record of transactions is also maintained separately on magnetic tapes to serve two purposes. First, as the transactions occur constantly, this record provides a link from one backup file to another. Second, as writing on magnetic disks occurs by overlying technique, the record of transactions helps in providing particulars of all records that caused a change to the magnetic disk file. In the case of system going down or the master file getting destroyed, the reconstruction can be carried out in the manner given below.

It has been assumed in the master file on magnetic disk got destroyed sometime during period 2. With the backup file on tape (which is a copy of the on-line master file at the end of period 1. And transaction records File, Which recorded all transactions during period 2, until the destruction of on-line master file), it becomes possible to reconstruct a new master disk. To do so, all master file data from backup magnetic tape file is written the new master disk file. Thereafter, all transactions from transaction file are processed against the magnetic disk master file, bringing the latter to the correct present stage.

b. Magnetic Tapes: The procedures followed in reconstruction of files in case of magnetic tapes is referred to as Generation Technique because files relating to two previous periods are retained in addition to the current updated master file and the current transaction file. The procedure operates as follows:

1. The master file produced is referred to as the son tape.
2. The son tape produced during the following updating run replaces the first 'son' tape, which becomes the father tape.
3. The next updating run produces a new 'son' tape (the present 'father' tape becomes 'grandfather' tape). The previous 'son' tape now becomes the 'father' tape.
4. On the next updating run, the original 'son' tape (now the 'grandfather' tape) is over written and can in fact be used for producing the new 'son' tape.

Backup Controls in the Database Environment: Since data sharing is a fundamental objective of the database approach, this environment is particularly vulnerable to damage from individual users. One unauthorized procedure, one malicious act, or one program error can lose the entire user community of its information resource. Also, because of data centralization, even minor disaster such as a disk failure can affect many or all users. When such events occur, the organization needs to reconstruct the database to pre-failure status. This can be done only if the database was properly backed up in the first place. Most DBMSs systems have a backup facility. This system provides four backup and recovery features: database backup, a transaction log. Check points, and a recovery module.

1. Back up: The backup feature makes a periodic backup of the entire database. This is an automatic procedure that should be performed at least once a day. The backup copy should then be stored in a secure remote area.

2. Transaction Log (Journal): The transaction log feature provides an audit trail of all processed transactions. It lists transactions in a transaction log file and records the resulting changes to the database in a separate database change log.

3. Checkpoint Feature: The checkpoint facility suspends all data processing while the system reconciles the transaction log and the database change log against the database. At this point, the system is in a "quite state". Checkpoints occur automatically several times an hour. If a failure occurs, it is usually possible to restart the processing from the last checkpoint. Thus, only a few minutes of transaction processing must be repeated.

4. Recovery Module: The recovery module uses the logs and backup files to restart the system after a failure.

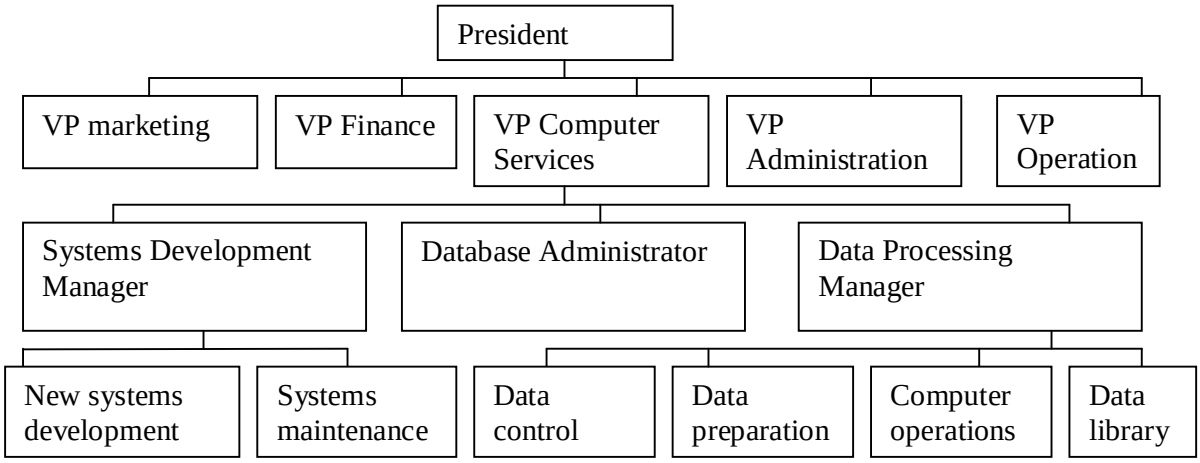
GENERAL CONTROLS: ORGANIZATION STRUCTURE CONTROLS

In a manual environment, operational tasks must be separated to:

1. Segregate the task of transaction authorization from transaction processing
2. Segregate record keeping from asset custody.
3. Divide transaction-processing tasks among individuals so that the perpetration of a fraud will require collusion between two or more individuals.

The tendency in a CBIS environment is to consolidate activities. A single application may authorize, process, and record all aspects of a transaction. Since transaction processing tasks are now performed by computer programs, the focus of segregation control shifts from the operational level to higher-level organizational relationships within the computer services function. The interrelationships among systems development, systems maintenance, data administration, and computer operations activities are of particular concern.

We will now examine organizational control issues within the context of the centralized model.



above figure contains an organizational chart of a centralized computer services function.

1. Separating Systems Development from Computer Operations: The segregation of systems development (both new systems development and maintenance) and operations activities is of the greatest importance. The relationship between these groups should be extremely formal, and their responsibilities should not be combined. Systems development and maintenance professionals should create (and maintain) systems for users. Operations staff should only run these systems and have no involvement in system design. Consolidating these functions invites fraud. With detailed knowledge of the application's logic and control parameters and access to computer functions, an individual could make unauthorized changes to the application during its execution. Such changes may be temporary and may disappear without a trace when the application terminates.

2. Separating the Database Administrator from Other Functions: Another important organizational control is the segregation of the database administrator function from other computer services functions. The DBA is responsible for a number of critical tasks pertaining to database security, including creating the database schema, creating user subschemas, assigning access authority to users, monitoring database usage, and planning for future expansion. Delegating these responsibilities to other persons who perform incompatible tasks threatens database integrity. The DBA function should be organizationally independent. There should be a separation of the DBA function from systems development also.

3. Separating new Systems Development from Maintenance: Some companies organize their systems development function into two groups: systems analysis and programming.

The systems analysis group works with the users to produce a detailed design of the new system. The programming group codes the program according to these design specification. Under this approach

the programmer who codes the original programs also maintains the system during the maintenance phase of the SDLC. Although a popular arrangement, this approach promotes two types of control problems: inadequate documentation and fraud.

a. Inadequate Documentation: Poor-quality systems documentation is a chronic problem for many firms. This is particularly true in companies that do not use CASE tools with automatic documentation features. There are basically two reasons for this. First, documenting a system is not as interesting as designing, testing, and implementing it. Systems professionals mostly prefer to move on to an exciting new project rather than document the one that has been completed. Pressure from users demanding new systems makes the decision to move on to something else even easier. The second reason for poor documentation is job security. When a system is poorly documented, it is difficult to interpret, test, and debug. Therefore, the programmer who understands the system (the one who coded it) is in a position of power and becomes relatively indispensable. However, when the programmer leaves the firm, a new programmer must maintain the system who is unfamiliar with it. The new programmer may have to study the detailed code of the application to gain an understanding of its logic. Depending upon the complexity of the system, the transition period can be long and costly.
b. *Program Fraud:* When the original programmer of a system also has maintenance responsibility, the potential for fraud is increased. Program fraud involves making unauthorized changes to program modules for purpose of committing all illegal acts.

4. An Alternative structure for system Development: The new systems development group is responsible for designing, programming, and implementing new systems projects. Upon successful implementation, responsibility for the system's ongoing maintenance falls to the systems maintenance group. This restructuring has implications that directly address the two control problems described previously.

First documentation standards are improved because the maintenance group requires documentation to perform its maintenance duties. Without complete and adequate documentation, the formal transfer of system responsibility from new systems development to systems maintenance simply cannot occur.

Second, denying the original programmer future access to the program prevents program fraud. Thus the fraudulent code, which is concealed within the systems, goes out of the programmer's control and may later be discovered. Hence, the risk associated with committing such program fraud increases. The success of this control depends on the existence of other controls that limit, prevent, and detect unauthorized access to programs (such as source program library controls) Organizational separation of functions alone cannot prevent such unauthorized access. However, they are critical to creating the environment in which unauthorized access can be prevented.

5. 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, such as magnetic tapes and removable disk packs. Access to the library should be controlled by a data librarian who is responsible for the receipt, storage, retrieval, and custody of data files. The librarian must keep a detailed log of each file, including file name, serial number, contents, creation date, and retention dates. The librarian issues scratch tapes (when their expiration dates are exceeded) to computer operators in accordance with system requests. When the program run is complete, the operator returns the file (s) to the librarian for storage.

The separation of the librarian from operations is important for the physical security of off-line data files. However, for many organizations, the volume of tape file usage is insufficient to justify a full-time librarian. The trend in recent years toward real-time and direct access batch systems has reduced the need for sequential tape storage. Thus, firms with modest tape usage-which still may represent

several hundred tape volumes-often, assign librarian functions to selected operators who perform these tasks on an ad-hoc basis in addition to their usual operator functions.

It is essential that operators who are assigned library tasks understand the control importance of this apparently mundane responsibility. Management should maintain strict control over who performs library functions to ensure that these responsibilities are not assumed by other operators during busy periods.

GENERAL CONTROLS: SYSTEM DEVELOPMENT CONTROLS

Controlling new systems development activities: The six activities discussed below deal with the authorization, development, and implementation of the original system.

System Authorization Activities: All systems must be properly authorized to ensure their economic justification and feasibility. As with any transaction, systems authorizations should be formal. This requires that each new system request be submitted in written form by users to systems professionals who have both the expertise and authority to evaluate and approve the request.

User Specification Activities: Users must be actively involved in the systems development process. User involvement should not be ignored because of a high degree of technical complexity in the system. Regardless of the technology involved, the user can create a detailed written description of the logical needs that must be satisfied by the system. The creation of a user specification document often involves the joint efforts of the user and systems professionals. However, it is most important that this document remain a statement of user needs. It should describe the user's view of the problem, not that of the systems professionals.

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 the user's needs. The scope of these activities includes systems analysis, general systems design, feasibility analysis, and detailed systems design. The adequacy of these activities is measure by the quality of the documentation that emerges from each phase. Documentation is both a control and evidence of control and is critical to the system's long term success.

Internal Audit Participation: The internal auditor plays an important role in the control of systems development activities, particularly in organizations whose users lack technical expertise. The auditor should become involved at the beginning 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 the maintenance phase.

Program Testing: All program modules must be thoroughly tested before they are implemented. The results of the tests are then compared against predetermined results to identify programming and logic errors.

Program testing is time-consuming, the principle task being the creation of meaningful test data. To facilitate the efficient implementation of audit objectives, test data prepared during the implementation phase must be preserved for future use. This will give the auditor a framework of reference for designing and evaluating future audit tests. For example, if a program has undergone no maintenance changes since its implementation, the test results from the audit should be identical to the original test results. Having a basis for comparison, the auditor can thus quickly verify of the program code. On the other hand, if changes have occurred, the original test data can provide evidence regarding these changes. The auditor can thus focus attention upon those areas.

User Test and Acceptance Procedures: Just before implementation, the individual modules of the system must be tested as a unified whole. A test team comprising user personnel, systems professionals, and internal audit personnel subjects the system to rigorous testing. Once the test team

is satisfied that the system meets its stated requirements, the system is formally accepted by the user departments.

The formal test and acceptance of the system are considered by many to be the most important control over the SDLC. It is imperative that user acceptance be documented. Before implementation, this is the last point at which the user can determine the system's adequacy and acceptability. Although discovering a major flaw at this juncture is costly, discovering the flaw during the production operations can be wasteful.

GENERAL CONTROLS: SYSTEMS MAINTENANCE CONTROLS

The last two controllable activities pertain to systems maintenance. On implementation, the system enters the maintenance phase of the SDLC. This is the longest period in the SDLC, often spanning several years. It is important to recognize that systems do not remain static throughout this period. Rather, they undergo substantive changes that constitute an amount many times their original implementation cost. The nature and extent of systems maintenance activities create great potential for exposure, which requires explicit control procedures.

Maintenance Authorization, Testing, and Documentation: Post implementation access to systems via maintenance activities increases the possibility of systems corruption. Logic may be corrupted either by the accidental introduction of errors or intentional acts to defraud. To minimize the potential exposure, all maintenance actions should require minimum four controls: formal authorizations, technical specifications, testing, and documentation updates. In other words, maintenance activities should be given essentially the same treatment as new development. The extent of the change and its potential impact on the system should govern the degree of control applied. When maintenance causes extensive changes to program logic, additional controls should be invoked, such as involvement by the internal auditor and the implementation of user test and acceptance procedures.

Source Program Library Controls: In larger computer systems, application program modules are stored in source code form on magnetic disks called the source program library (SPL).

The Worst Case Situation- No Controls: A SPL without controls has the potential to create two serious forms of exposure:

1. Access to program is completely unrestricted: Programmers and others can access any programs stored in the library, and there is no provision for detecting an unauthorized intrusion.
2. Because of these control weaknesses, programs are subject to unauthorized changes. Hence, there is no basis for relying on the effectiveness of other controls (maintenance authorization, program testing, and documentation). In other words, with no provision for detecting unauthorized access to the SPL, the program's integrity cannot be verified.

A controlled SPL environment: To control the SPL, protective features and procedures must be explicitly addressed. This requires the implementation of an SPL management system (SPLMS).

This 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.

SPLMSs may be supplied by the computer manufacturer as part of the operating system or may be purchased through software vendors. Some organizations develop their own SPL software to provide special control features. However, mere presence of SPLMS does not guarantee program integrity. An SPL requires specific planning and control techniques to ensure program integrity. The control

techniques discussed below address only the most vulnerable areas and should be considered minimum SPL controls.

Password Control: One form of access control over the SPL is provided by assigning passwords. Every financially significant program stored in the SPL can be assigned a separate password. As previously discussed, passwords have drawbacks. When more than one person is authorized to access a program, preserving the secrecy of a shared password is a problem.

Separation of Test Libraries: Another approach for an improvement on the shared password approach through the creation of separate password-controlled library (or directories) for each programmer. Under this concept, a strict separation is maintained between the production programs that are subject to maintenance in the SPL and those being developed. Production programs are copied into the programmer's library for maintenance and testing purposes only. Direct access to the production SPL is limited to a specific librarian group that must approve all requests to modify, delete, and copy programs. Passwords for production programs can be changed regularly and disclosed only on a need-to-know basis.

Audit Trail and Management Report: An important feature of SPL management software is the creation of reports that enhance management control and the audit function. The most useful of these are program modification reports, which describe in detail all program changes (additions and deletions) to each module. These reports should be part of the documentation file of each application to form an audit trail of program changes over the live of the application. During an audit, these reports can be reconciled against program maintenance requests to verify that only the required changes were actually implemented. For example, if a programmer attempted to use a legitimate maintenance action as an opportunity to commit program fraud, the unauthorized code changes would be presented in the program modification reports. These reports can be produced as hard copy and on disk and can be governed by password control, thus limiting access to management and auditors only.

Program Version Number: The SPLMS assigns a version number automatically to each program stored on the SPL. When programs are first placed in the libraries (at implementation), they are assigned a version number of zero. With each modification to the program, the version number is increased by one. For instance, after five authorized maintenance changes, the production program will be version 05. This feature, when combined with audit trail reports, provides evidence for identifying unauthorized changes to program modules. An unauthorized change is signaled by a version number on the production load module that can not be reconciled to the number of authorized changes. For example, if ten changes were authorized but the production program is Version 12, then one of two possibilities explains this discrepancy: 1. Authorized changes occurred that are unsupported by documentation or (2) unauthorized changes were made to the program that increased the version numbers.

Controlling Access to Maintenance Commands: Powerful Maintenance commands are available for most library systems that can be used to alter or eliminate program passwords, alter the program version (modification) number, and temporarily modify a program without generating a record of the modification.

There are a number of legitimate technical reasons why systems designers must sometimes use these commands. However, if not controlled, maintenance commands open the possibility of unrecorded, and perhaps unauthorized program modifications. Hence, access to the maintenance commands themselves should be password controlled, and the authority to use them should be controlled by management or the security group.

Message Sequence Numbering: An intruder in the communications channel may attempt to delete a message from a stream of messages, changes the order of messages received, or duplicate a message.

Through message sequence numbering, a sequence number is inserted in each message, and any such attempt will become apparent at the receiving end.

GENERAL CONTROLS: COMPUTER CENTRE SECURITY AND CONTROL

Although a breach of computer security can take many forms, they can be categorized as accidental or incidental. Accidental breach of security is a greater threat than incidental breach. Accidental breach of security due to such natural calamities as fire, flood and earthquake etc. may cause total destruction of important data and information. Incidental or fraudulent modification or tempering of financial records maintained by the organization can cause considerable amount of money to be disbursed to fraudulent personnel. Hence, there is a great need to ensure the security of computer system, also proper safeguards should be devised. Such safeguards include arrangement for fire detection and fire-avoiding equipment, security from water damage, structural damage and pollution damage and unauthorized intrusions on computer equipment, alternative arrangements at other computer centres to meet emergency requirements, alternative and uninterrupted power supply arrangement and hardware insurance in case of owned equipment. Some of the common accidental damages to the system are discussed:

Fire damage: Fire is often the major threat to the physical security of a computer installation. Loss from fire can be substantial. In a number of computer installations of very large organizations, fire has destroyed hardware and software worth of million of rupees. Some countries have various public services and government organizations that provide advice on fire production measures. However, the implementation of specific system usually requires specialist's advise. Some major features of a well designed fire protection system are briefly discussed below:

1. Both automatic and manual fire alarms are placed at strategic locations throughout the installation.
2. Companies have a choice of either highly sophisticated electronic fire detection equipment or low-tech fire extinguishers. Sprinkler systems are recommended when a computer room contains an considerable amount of combustible material. It may be noted here that some people have misconception about sprinklers. They think that water will permanently harm the equipment. However, this is not the case. Equipment will not be damaged by water if is first de-energized. In case, the equipment gets wet, it can be made functional again by dissembling it, drying it out and putting it back together again. However, in this process the time will be lost, in cleaning up and drying out the equipment which may vary from one day to several weeks depending upon the equipment and the amount of water that is used.

   An alternative means is halogen gas, which requires no clean up. One has to just exhaust the room and the halogen gas disappears from the room. However, halogen gas equipment is far more expensive than water sprinkler.

   All these systems can be controlled by a micro processor fire detection systems, which can be designed and programmed to respond for smoke. This system can be programmed to shut down computer equipment and air conditioners as soon as smoke is detected, and also to charge sprinkler system or set off halogen gas.
3. An appropriate type of normal fire extinguishers may be placed at strategic locations through out the installation.
4. A control panel may be installed which shows where in the installation an automatic or manual alarm has been triggered.
5. Besides the control panel, master switches may be installed for power (including air conditioning) and automatic extinguisher system.
6. The building may be constructed from fire resistant materials and it should be structurally stable when fire damage occurs.
7. Fire extinguishers and fire exits should be marked clearly.
8. When a fire alarm is activated, a signal may be sent automatically to a permanently manned station.

The security officer should arrange regular inspection of fire protection systems. Proper use of these systems requires staff training periodic drills. Hence, all the staff members should be make aware of how to use these systems. The procedures to be followed during an emergency should be properly documented.

Water damage: Water damage to a computer installation can be the outcome of a fire; the specific system sprays water that enters hardware or water pipes may burst. Water damage may also result from other resources such as cyclones, tornadoes etc. some of the major ways of protecting the installation against water damage are as follows:

1. Wherever possible have water proof ceilings, walls and floors.
2. Ensure an adequate drainage system exists.
3. Install alarms at strategic points within the installation.
4. In flood areas have the installation above the high water level.
5. Have a master switch for all water mains.
6. Use a dry pipe automatic sprinkler system that is charged by an alarm and activated by the fire.
7. Cover hardware with a protective fabric when it is not in use.

Energy variations: Energy variations take the form of increases in power, decreases in power or loss of power. Voltage regulators protect hardware against temporary increase in power; circuit breakers protect the hardware against sustained increase. Battery back up can be provided in case a temporary loss of power occurs. However, a generation plant is needed for sustained losses in power. The level of protection needed depends on the company's ability to maintain an uninterrupted power source.

Pollution damage: the major pollutant is dust which arises if there is inadequate filtering of air passing through air conditioning system or if it is allowed to accumulate on equipment, floors etc. while working on computer site preparation, considerations should be given to ensure dust-free environment in the computer room. Only such materials and finishing may be used inside the room which enable it to remain dust free. Dust caught between the magnetic tape/disk and the reading and writing heads on a tape/disk, in addition to permanently damaging the media, can cause reading and writing errors. Dust between the surface of a magnetic disk and the heads may cause the head to score the recording surface. Several steps can be taken to avoid polluting the installation. Regular cleaning of ceilings, walls, floors, storage cabinets and equipment is necessary. Vacuuming is especially important, particularly in areas where dust collects. Dust collecting rugs can be placed at entrances. Floors can be treated with special antistatic compounds, food stuff can be prohibited in computer room. Regular emptying of wastepaper baskets prevents dust from collecting.

Unauthorized intrusion: Unauthorized intrusion takes two forms. The intruder physically may enter the installation to steal assets or carry out damage. Alternatively, the intruder may eavesdrop on the installation by wire-tapping, installing an electronic bug or using a receiver that picks up electro-magnetic signals. Physical intrusions may be prevented by restricting the entry of personnel to the computer centre. Alarms and guards may be used to detect an unauthorized intruder. There are various types of security devices and systems that signal the presence of an intruder. A badge system may be used to identify the status of personnel within the installation: permanent staff or visitors. All visitors should be escorted by a permanent staff member. Security check might be performed before a visitor is issued a badge.

Eavesdropping breaches the privacy of data. It may be used by an intruder to obtain a password or sensitive information of the organization. Various devices are available to detect the presence of bugs. The security administrator periodically may employ a security firm that possesses these devices to examine the installation.

Disaster Recovery Plan: Some disasters can not be prevented or avoided. The survival of a firm affected by such a disaster depends on how it reacts. With careful planning, the full impact of a disaster can be absorbed and the organization can still recover.

The term *"Disaster Recovery"* describe the contingency measures that organisations have adopted at key computing sites to recover from, or to prevent any enormously bad event or disaster. The primary objective of a disaster recovery plan is to assure the management that normalcy would be restored in a set time after any disaster occurs, thereby minimising losses to the orgnization.

Although each organization would like to have a specifically tailored disaster recovery plan, the general components of the plan would be as follows:

1. **Emergency Plan:** This part of the Disaster Recovery Plan (DRP) outlines the actions to be undertaken immediately after a disaster occurs. It identifies the personnel to be notified immediately, for example, fire service, police, management, insurance company etc. it provides guidelines on shutting down equipment, termination of power supply, removal of storage files and removable disks, if any. It sets out evacuation procedures like sounding the alarm bell, activating fire extinguishers, evacuation of personnel. It also provides return procedures as soon as the primary facility is ready for operation like backing up data files at off-site, deleting data from disk drives at third party's site, relocation of proper versions of backup files, etc.

2. **Recovery Plan:** This part of the DRP sets out how the full capabilities will be restored. A recovery committee is constituted. Preparing specifications of recovery like setting out priorities for recovery of application systems, hardware replacement etc. will be the responsibility of Recovery Committee.

   The following steps may be carried out under this plan:
   1. An inventory of the hardware, application systems, system software, documentation etc. must be taken.
   2. Criticality of application systems to the organization and the importance of their loss must be evaluated. An indication must be given of the efforts and cost involved in restoring the various application systems.
   3. An application systems hierarchy must be spelt out. This would be used when the management decides to accept a degraded mode of operation.
   4. Selection of a disaster recovery site must be made. A reciprocal agreement with another organization having compatible hardware and software could be made. However, systems availability an data security problems must be considered at this point. Hiring a service bureau is another option. If the situation warrants, a fully operational backup site could also be considered.
   5. A formal backup agreement with another company must be made. This should cover the periodical exchange of information between the two sites regarding changes to hardware/software, the time and duration of systems availability, modalities of testing the plan etc.

3. **Backup Plan:** Organizations no matter how physically secure, their systems are always vulnerable to the disaster. Therefore, an effective safeguard is to have a backup of anything that could be destroyed, be it hardware or software. As regards hardware, stand by, as discussed above, must be kept with regard to the needs of a particular computer environment. So far as the software is concerned, it is necessary to make copies of important programs, data files, operating systems and test programs etc. in order to get back into operation before the company can suffer an intolerable loss. Often, the originals are stored at site that is physically distant from the actual site, and where duplicate copies are used for processing. The backup copies must be kept in a place which is not susceptible to the same hazards as the originals.

4. **Test Plan:** This plan looks after the testing of DRP and analysis of the result. It identifies deficiencies in the emergency, backup or recovery plan. It contains procedures for conducting DRP testing like

    1. Paper walk-through: It involves critical personnel in the plan's execution, reasoning out what might happen in the even of different disasters.
    2. Localized tests: it simulates system crash. This test is performed on different aspects of DRP.
    3. Full operational test: It is nearer to disaster conditions. Paper walkthrough and localised tests should have been conducted before completely shutting down the operations to simulate disasters.

Disaster recovery and reconstruction:
It includes the following:

- Retrieving critical and vital data, programs from off-site storage
- Installing and testing systems software and applications
- Operating from off-site
- Rerouting network communication traffic
- Reconstruction of data bases
- Maintaining supply of necessary office goods (stationary etc.)

DRP TESTING : The test should try to do the following:

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

The test execution includes post-test which is the clean-up of activities like returning all resources to their proper places, deleting of company data from 3rd party system. Results are documented, result analysis is done in terms of time taken for doing the various tasks, amount of work done at the backup site, cost of critical systems that were successfully recovered and accuracy of actual processing cycle.

Insurance: Risk to computer system can be controlled through system design, installation of security measures and regular security audit. However, some residual risks always exists that can not be covered. One way of handling this residual is to transfer it contractually to a third party by way of insurance of the computer installation.

If a decision is made to purchase insurance cover, management must be careful to ensure that they consider all major potential losses; the replacement cost of purchased or leased hardware must be covered, special construction relating to raised floors and air conditioning must be covered etc. the types of insurance policies that might be obtained are:

1. Data processing policy
2. Valuable papers and records policy
3. Business interruption insurance
4. Extra expense insurance.
5. Errors and omissions insurance.

GENERAL CONTROLS: INTERNET AND INTRANET CONTROLS

Communication subsystem is responsible for transmitting data among all the other subsystem within a system or for transmitting data to or receiving data from other system. Physical manifestation may be a cable linking a disk drive with a central processor or a configuration of minicomputers communication lines linking remote computer that must interact with each other.

There are two major exposures in the communication subsystem. First, data may be lost or corrupted through component failure. Second, a hostile party (intruder) may seek to subvert data being transmitted through the subsystem.

Component failure: The primary components in the communication subsystem are—

a. Communication lines viz., twisted pair, coaxial cables, fiber optics, microwave, satellite.
b. Hardware—ports, modems, multiplexers, switches, repeaters and
c. Software-packet switching software, polling software, data compression software.

Due to component failure, transmission between sender and receiver can be disrupted, destroyed, or corrupted in the communication system. Equipment failure can also result in the loss of databases and program stored on the network server.

Subversive threats: An intruder attempts to violate the integrity of some components in the subsystem.

a. Invasive tap: By installing it on communication line, he can read & modify data.
b. Inductive tap: It monitors electromagnetic transmissions and allows the data to be read only.

Subversive attacks can provide intruders with important information about messages being transmitted. They can manipulate messages as stated below.

1. Intruders may insert a message in a message stream being transmitted, eg., EFTs add transfer of funds in the an additional account.
2. Intruders may delete a message being transmitted eg. Remove a/c withdrawal message.
3. Intruders may modify the contents of a message. They may increase the amount filled in a deposit transaction.
4. Intrudes may alter the order of the messages in a message stream.
5. Duplicate messages in a message stream eg. They may copy deposit transactions for their accounts.
6. Intruders may deny message services between a sender and a receiver by discarding messages or delaying messages.
7. Intruders may use techniques to establish spurious associations so that they are regarded as legitimate users of a system. They may play back a handshaking sequence previously used by a legitimate user of the system.

Controlling risk from Subversive Threats

a. Firewalls: Organizations connected to the Internet or other public networks often implement an electronic "firewall" to insulate their Intranet from outside intruders. A firewall is a system that enforces access control between two networks. To accomplish this:

- All traffic between the outside network and the organization's Intranet must pass through the firewall.
- Only authorized traffic between the organization and the outside, as specified by formal security policy, is allowed to pass through the firewall.
- The 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 or her level of access authority, and then direct the user to the program, data, or service requested. In addition to insulating the organization's network from external networks, firewalls can also be used to insulate portions of the organization's Intranet from internal access. There are a number of firewall products on the market. Firewalls can be grouped into two general types: network-level firewalls, and application-level firewalls.

Network-level firewalls provide low cost and low security access control. This type of firewall consists of screening router that examines the source and destination addresses that are attached to incoming message packets. The firewall accepts or denies access requests based on filtering rules that have been programmed into it. Similar to an intelligent PBX, the firewall directs incoming calls to the correct internal receiving node. Network-level firewalls are insecure because they are designed to facilitate the free flow of information rather than restrict it. This method does not explicitly

authenticate outside users. Using IP spoofing, hackers can disguise their message packets to look as if they came from an authorized user and thus gain access to the host's network.

Application-level firewalls provide a high level of customizable network security, but can be extremely expensive. These systems are configured to run security applications called proxies that permit routine services such as e-mail to pass through the firewall, but can perform sophisticated functions such as logging or user authentication for specific tasks. If an outside user attempts to connect to an unauthorized service or file, the network administrator or security group can be notified immediately.

b. Controlling Denial of Service Attacks: When a user establishes a connection on the Internet through TCP/IP, a three-way handshake takes place. The connecting server sends an initiation code called a SYN packet to the receiving server. The receiving server then acknowledges the request by returning a SYN/ACK packet. Finally, the initiating host machine responds with an ACK packet code. Computer hackers and crackers have devised a malicious act called a denial of service attack, in which the attacker transmits hundreds of SYN packets to the targeted receiver but never responds with an ACK to complete the connection. As a result, the ports of the receiver's server are clogged with incomplete communication requests that prevents legitimate transactions from being received and processed.

If the target organization could identify the server that is launching the attack, the firewall could be programmed to ignore all communication from that site. Such attacks, however, are difficult to prevent because IP spoofing is used to disguise the source of the message. IP spoofing programs that randomise the source address of the attacker have been written and publicly distributed over the Internet. Therefore, to the receiving site it appears that the transmissions are coming from all over the Internet.

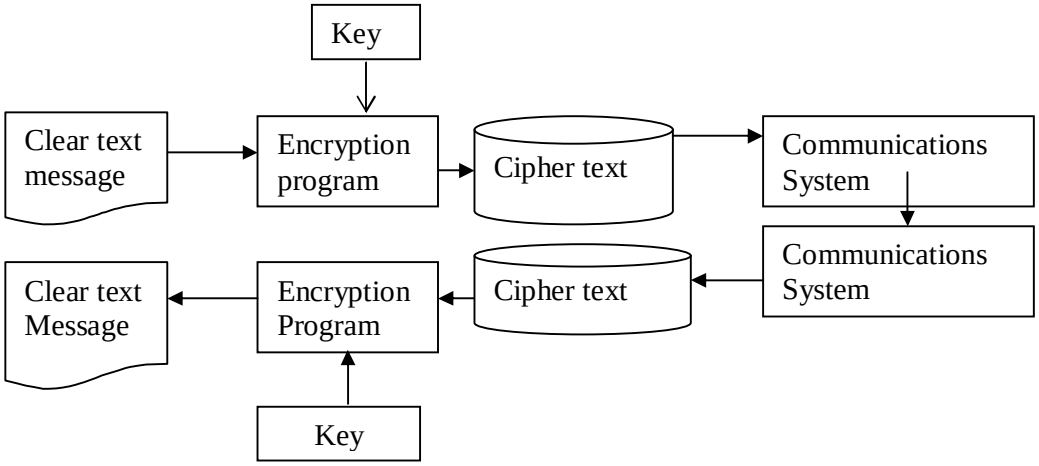
Denial of service attacks can severely hamper an organization's ability to use the Internet to conduct commerce. Although this activity cannot currently be prevented, there are two actions that management and accountants can take to limit the exposure. First, Internet sties with firewalls must engage in a policy of social responsibility. The firewalls at the source site can be programmed to block messages with non-internal addresses. This assures the organization's management that no undetected attack could be launched from its site. This strategy will not, however, prevent attacks from areas of the Internet that do screen outgoing transmissions.

Second, security software is available for the targeted sites that scan for half open connections. The software looks for SYN packets that have not been followed by an ACK packet. The clogged ports can than restored to allow legitimate connections to be made.

c. Encryption: Encryption is the conversion of data into a secret code for storage in databases and transmission over networks. The discussion here pertains to transmitted data, but these basic principles apply also to stored data. The sender uses an encryption 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 that is typically from 56 to 128 bits in length. The more bits in the key, the stronger the encryption method. Today, nothing less than 129 bit algorithms are considered truly secure. Two general approaches to encryption are private key and public key encryption.

Private Key Encryption: Data encryption standard (DES) is a private-key encryption technique designed in the early 1970s by IBM. The DES algorithm uses a single key known to both the sender and the receiver of the message. To encode a message, the sender provides the encryption algorithm with the key, which is used to produce a cipher text message. The message enters the communication channel and is transmitted to the receiver's location where it is stored. The

receiver decodes the message with a decryption program that uses the same key employed by the sender. Given below figure illustrate this technique.



The primary problem with the DES approach is that a perpetrator may discover the key and intercept and decipher the message. The more individuals who need to know the key, the greater the probability of it falling into the wrong hands.

Public key encryption: The public key encryption techniques use two different keys: one for encoding messages and the other for decoding them. Each recipient has a private key that is kept secret and a public key that is published. The sender of a message uses the receiver's public key to encrypt the message. The receiver then uses his or her private key to decrypt the message. Users never need to share their private keys to decrypt messages, thus reducing the likelihood that they fall into the hands of a criminal.

d. Message transaction Log: An intruder may successfully penetrate the system by trying different password and user ID combinations. Therefore, all incoming and outgoing messages, as well as attempted (failed) access, should be recorded in a message transaction log. The log should record the user ID, the time of the access, and the terminal location or telephone number from which the access originated.

e. Call Back Devices: As we have seen, networks can be equipped with security features such as passwords, authentication devices, and encryption. The common weakness to all of these technologies is that they impose the security measure after the criminal has connected to the LAN server. Many feel that the key to network security is to keep the intruder off the LAN to begin with.

A call-back device requires the dial-in user to enter a password and be identified. The system then breaks the connection to perform user authentication. If the caller is authorized, the call-back device dials the caller's number to establish a new connection.

This limits access from only authorized terminals or telephone numbers and prevents an intruder masquerading as a legitimate user.

GENERAL CONTROLS: PERSONAL COMPUTER CONTROLS

The capabilities, adaptability and user friendliness of Personal Computers (PC's) are posing a serious challenge to auditors. PC's have the following special characteristics which give rise to new risks.

- They are small, fast, and powerful. Some of them even approach the power of minis and mainframes.
- They are available in many makes and models.
- Floppies provide a convenient way of data storage.
- Their user-friendliness has resulted in end-user computing.
- They act as inexpensive front-ends to large computers.
- There is a tendency to buy off-the shelf application packages.
- They are prone to virus infection.

The resultant new security risks are as follows:

- PC's are likely to be shifted from one location to another or even taken outside the organization.
- Decentralized purchasing of PC's can result in hardware/software incompatibility in the long run.
- Floppies can be very conveniently transported from one place to another, as a result of which data corruption may occur. Mishandling, improper storage etc. can also cause damage.
- The inherent data security provided is rather poor.
- There is a chance that applications software are not thoroughly tested.
- Segregation of duties is not possible, owing to limited number of staff.
- The operating staff may not be adequately trained.
- Computer viruses can slow down the system, corrupt data and so on.

The Security measures that could be exercised are as follows:

- Physically locking the keyboard or the PC itself must be enforced.
- Proper logging of equipment shifting must be done.
- The PC purchases must be centrally coordinated and company-wide standards established for spread sheets, word-processors, applications software etc.
- Floppies must be stored in secured places and their issues duly authorized. They must be adequately packed before any shipment.
- Data and programs on hard-disks must be secured using hardware/software mechanisms. Backups must be taken regularly.
- Minimum standards must be set for developing, testing and documenting applications.
- Properly organized training programs must be periodically conducted. More than one user should be trained on each application.
- Virus prevention and detection software obtained from reliable sources must be used. Write protect tabs should be used on diskettes that do not require any alteration. Pirated software should be strictly avoided.
- The PC's and their peripherals must be maintained regularly.

While the proliferation of powerful PC's in recent years has its own plus points, the associated risks must not be ignored. Thus, implementing effective controls is of prime importance.

Some other inherent problems of personal computers and the controls to be exercised are discussed below:

Weak Access Control: Security software that provides log-on procedures is available for PCs. Most of these programs, however, become active only when the computer is booted from the hard drive. A computer criminal attempting to circumvent the log-on procedure may do so by forcing the computer to boot from the A: drive, where by an uncontrolled operating system can be loaded into the computer's memory. Having bypassed the computer's stored operating system and security package, the criminal has unrestricted access to data and programs on the hard disk.

Disk locks are devices that prevent unauthorized individuals from accessing the floppy disk drive of a computer. One form of disk lock is a memory-resident program that prevents the computer from being booted from the A: drive. The lock will also prevent the A: drive from being used to run programs, upload data and programs to the hard disk, or download from the hard disk. This form of disk lock is password controlled so it can be disabled as needed by an authorized user.

Multilevel Password Control: It is used to restrict employees who are sharing the same computers to specific directories, programs, and data files. This technique uses stored authorization tables to further limit an individual's access to read-only, data input, data modification, and data deletion capability. Multilevel password control can greatly enhance the small organization's control environment.

Inadequate Backup Procedures: To preserve the integrity of mission-critical data and programs, organizations need formal backup procedures. Adequate backup of critical files is actually more difficult to achieve in simple environments than it is in sophisticated ones. In mainframe and network environments, backup is controlled automatically by the operating system, using specialized software and hardware. The responsibility of providing backup in the PC environment falls to the user. Often, because of lack of computer experience and training, users fail to appreciate the importance of backup procedures until it is too late.

Computer failure, usually disk failure, is the primary cause of significant data loss in the PC environment. If the hard drive of the microcomputer fails it may be impossible to recover the data stored on the disk. Formal procedures for making backup copies of critical data (and program) files can reduce this threat considerably.

Floppy Disk Backup: Files can be backed up to floppy disks at routine periods during processing and stored away from the computer. In the event of a microcomputer failure, the data file can be reconstructed from the backup disks. This requires a conscious effort on the part of the user. Failure to back up data even one time can result in its loss.

Dual Internal Hard Drives: Microcomputers can be configured with two physical internal hard disks. One disk can be used to store production data while the other stores the backup files. A batch program, run prior to or immediately after each data processing session, can copy the data file to the backup disk. Thus, backup is almost transparent to the user and involves a minimum of effort. This is a useful technique for the backup of large files that cannot be stored effectively on floppy disks. If one of the internal hard drives fails, the data files can be retrieved from the remaining hard drive.

External Hard Drives: A popular backup option is the external hard drive with removable disk cartridge, which can store more than a gigabyte of data per cartridge. When a cartridge is filled, the user can remove it and insert a new one. External hard drives can be used as an effective and simple back technique.

Tape Backup Devices: The most common type of archive device for PCs is magnetic tape. These may be internal or external devices and provide efficient and inexpensive backup. In normal backup mode, a single tape can store about 1.6 gigabytes of data. In compressed mode, a tape can store up to 3.2 gigabytes.

CHAPTER 14

CONTROLS IN EDP SET-UP: APPLICATION CONTROLS

INTRODUCTION

Application controls deal with exposures within specific application, such as payroll, purchases, and cash disbursements. Application controls, which may be manual actions or procedures programmed into an application, fall into three broad categories input controls, processing controls, and output controls

INPUT CONTROLS

The data collection component of the information system is responsible for bringing data into the system for processing. Input controls at this stage attempt to ensure that these transactions are valid, accurate, and complete. Data input procedures can be either source document-triggered or direct input.

Classes of Input Control: Input controls are divided into the following broad classes:

- Source document controls
- Data coding controls
- Batch controls
- Validation controls
- Input error correction
- Generalized data input systems

Source Document Controls: In systems that use physical source documents to initiate transactions, careful control must be exercised over these instruments. Source document fraud can be used to remove assets from the organization. For example, an individual with access to purchase orders and receiving reports could fabricate a purchase transaction to a non-existent supplier. If these documents were entered into the data processing stream, along with a fabricated vendor's invoice, the system could process these documents as if a legitimate transaction taken place. In the absence of other compensating controls to detect this type of fraud, the system would create an account payable and subsequently write a cheque for payment.

To control against this type of exposure, the organization must implement control procedures over source documents to account for each document, as described below.

1. *Use Prenumbered Source Documents:* Source documents should come prenumbered from the printer with a unique sequential number on each document. Source document numbers permit accurate accounting of document usage and provide an audit trail for tracing transactions through accounting records.
2. *Use source Documents in Sequence:* Source documents should be distributed to the users and used in sequence. This requires that adequate physical security be maintained over the source document inventory at the user site. When not in use documents should be locked away. At all times, access to source documents should be limited to authorized persons.
3. *Periodically audit Source Documents:* Missing source documents should be identified by reconciling document sequence numbers. Periodically, the auditor should compare the number of documents used to date with those remaining in inventory plus those voided due to errors. Documents not accounted for should be reported to management.

Data Coding Controls: Coding controls are checks on the integrity of data codes used in processing. A customer's account number, an inventory item number, and a chart of accounts numbers are all examples of data codes. Two types of errors can corrupt a data code and cause processing errors: transcription, and transposition.

Transcription errors fall into three classes:

1. *Addition errors* occur when an extra digit or character is added to the code. For example, inventory item number 83276 is recorded as 832766.
2. *Truncation errors* occur when a digit or character is removed from the end of a code. In this type of error, the inventory item above would be recorded as 8327.
3. *Substitution errors* are the replacement of one digit in a code with another. For example, code number 83276 is recorded as 83266.

There are two types of **transposition errors.** *Single transposition errors* occur when two adjacent digits are reversed. For instance, 83276 is recorded as 38276. *Multiple transposition errors* occur when nonadjacent digits are transposed. For example, 83276 is recorded as 87236.

Any of these errors can cause serious problems in data processing if they go undetected. For example, a sales order for customer 732519 that is transposed into 735219 will be posted to the wrong customer's account. A similar error in an inventory item code on a purchase order could result in ordering unneeded inventory and failing to order inventory that is needed. These simple errors can severely disrupt operations.

Check digits: One method for detecting data coding errors is a check digit. A check digit is a control digit 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, as a prefix, a suffix, or embedded someplace in the middle. Whenever the code is transcribed from one document to another this check is to be effected. Consider the number 3721 for example. The weightage as below are assigned to its various positions. Other steps to derive the check digit are also given.

Step 1:	3	7	2	1
Weightage	5	4	3	2

Step 2: 1*2+2*3+7*4+3*5=51
Step 3: 51%11=4 with a remainder of 7.
Step 4: check digit =11-7=4.

The check digit may be placed at the end of the number, giving 37214. (If the check digit turns out to be 10, letter A may be taken as the equivalent).

When the number is checked for validity the following steps would be gone over.

Step 1: 4*1+1*2+2*3+7*4+3*3=55
Step 2: 55%11 = 5 with a remainder 0.

If the number had been mispunched as 73214 and remainder of 4 (and not 0) would be obtained, thereby causing an error message. The check digit described above is known as the **11-module check digit** for the reasons which should be apparent now. It is to be noted that on some errors, the check digit may fail us. There are numerous other check digit schemes but the 11-module check digit scheme has been empirically established as the best to detect the transposition errors commonly encountered in data processing situations.

Batch controls: Batch controls are an effective method of managing high volumes of transaction data through a system. The objective of batch control is to reconcile output produced by the system with the input originally entered into the system. This provides that:

- All records in the batch are processed.
- No records are processed more than once.
- An audit trail of transactions is created from input through processing to the output stage of the system.

Batch control is not exclusively an input control technique. Controlling the batch continues through all phases of the system.

Achieving batch control objectives requires grouping similar types of input transactions together in batches and then controlling the batches throughout data processing. Two documents are used to accomplish this task: a batch transmittal sheet and a batch control log. The batch transmittal sheet captures relevant information about the batch, such as:

1. A unique batch number.
2. A batch date.
3. A transaction code (indicating the type of transactions, such as a sales order or cash receipt).
4. The number of records in the batch (record count).
5. Total amount value of a financial field (batch control total).
6. The total of a unique non-financial field (hash, total).

Usually, the batch transmittal sheet is prepared by the user department and is submitted to data control along with the batch of source documents. Sometimes the data control clerk acting as a liaison between the users and the data processing department, prepares the transmittal sheet.

The data control clerk receives transactions from users assembled in batches of 40 to 50 records, the clerk assigns each batch a unique number, date-stamps the documents, and calculates the batch control numbers, such as the total amount of the batch and a hash total(discussed later). The clerk enters the batch control information in the batch control log and submits the batch of documents, along with the transmittal sheet, to the data entry department.

The data entry group codes and enters the transmittal sheet data onto the transaction file, along with the batch of transaction records. The transmittal data may be added as on additional record in the file or placed in the file's internal trailer label. The transmittal sheet becomes the batch control record and is used to assess the integrity of the batch during processing. For example, the data entry procedure will recalculate the batch control totals to make sure that the batch is in balance. For example, suppose that the transmittal record shows a batch of 50 sales order records with a total value of Rs. 122,674,87 and a hash total of 4537838. At various points throughout and at the end of processing, these amounts are recalculated and compared to the batch control record. If the procedure recalculates the same amounts, the batch is in balance.

After processing, the output results are sent to the data control clerk for reconciliation and distribution to the user. The clerk updates the batch control log to record that the processing of the batch was complete successfully.

Hash Totals: The term hash total, refers to a simple control technique that uses non-financial data to keep track of the records in a batch. Any key field, such as a customer's account number, a purchase order number, or an inventory item number, may be used to calculate a hash total.

Let's see how his seemingly meaningless number can be of use. Assume that after this batch of records leaves data control, but prior to data input, someone replaced one of the sales orders in the batch with a fictitious record of the same rupee amount. How would the batch control procedures detect this irregularity? Both the record count and the rupee amount control totals would be unaffected by this act. However, unless the perpetrator obtained a source document with exactly the same sales order number (which would be impossible, since they should come uniquely pre-numbered from the printer), the hash total of sales order number calculated by the batch control procedures would not balance. Thus, the irregularity would be detected.

Validation Controls: Input validation controls are intended to detect errors in transaction data before the data are processed. Validation procedures are most effective when they are performed as close to the source of the transaction as possible. However, depending on the type of Computer

Based Information Systems (CBISs) in use, input validation may occur at various points in the system.

Some validation procedures are performed by each processing module prior to updating the master file record.

There are three levels of input validation controls:
a. Field interrogation
b. Record interrogation
c. File interrogation

a. *Field Interrogation:* Field interrogation involves programmed procedures that examine the characters of the data in the field. The following are some common types of field interrogation.

Limit checks: Applied to both the input data and the output data. The field is checked by the program to ensure that its value lies within certain predefined limits (in the program). This applies to both input and output fields considered to be important. Several examples follow:

Picture Checks: These check against entry into processing of incorrect characters.

Example: All department numbers may be made up of numeric. An incorrect dept. No. 4D3 would thus be filtered.

Valid code Checks: Checks are made against predetermined transactions codes, tables or order data to ensure that input data are valid. The predetermined codes or tables may either be embedded in the programs or stored in files.

Example: In an inventory updating application, the following may be comprehensive list of transaction codes:

I = Issue
R = Receipts
C = Allocations against customer orders
A = Amendments
D = Deletion
N = Addition of new records
S = Stock taking adjustments.

Any other code would be brought out in the error message.

Check Digit: As discussed in previous section.
Arithmetic checks: Arithmetic is performed in different ways to validate the result of other computations of the values of selected data fields.
Example The discounted amount for Rs. 4,000 at 5% discounted may be computed twice by the following different ways:

4,000 - 4,000*5/100 = 3,800 or

4,000 ((100-5)/100) = 3,800.

Cross Checks may be employed to verify fields appearing in different files to see that the result tally. For example, the quantity received, quantity invoiced by the supplier and quantity ordered may be compared. Incidentally, it may also be necessary to effect a check on the units of

quantity. Fraud is possible if the unit is gun on the transaction whereas the standard unit in the master file is Kg.

b. Record integration

Sequence checks are exercised to detect any missing transaction, off serially numbered vouchers (subsequently transcribed for computer processing) or erroneous sorting.

Format completeness checks are used to check the presence and position of all the fields in a transaction. This check is particularly useful for variable data field records.
Redundant data checks are used in sequential processing. Matching keys of the transaction record and its master record may not be deemed enough. One may, in a sales application for example, want to compare, say first five characters of the customer's name.
Combination checks: Credit against shipments is invalid and ought to be rejected. As another example, consider the following set of codes:

Type of Transaction	Type of Customer
A (Payment on Credit)	1 (Individual)
B (Cash payment)	2 (Regular)
	3 (Regular-Bulk)

In theory, there are 6 combinations, but, in practice, such combinations as A1 could be invalid.

Passwords: These are issued to the various users in on-line systems for processing their inquiries. For example, the finance manager may have to enter via the terminal his code no., his name and say, the height of his son which was issued to him as his password. The program will compare this against the table of passwords so that any fraudulent attempt by any other employee to retrieve sensitive financial data is frustrated. It is desirable to periodically change the passwords.

Once a user has been identified in an on-line system, it remains to be seen what he is authorized to access, read, write etc.

Cost benefit analysis must be made for each check. For example, noting one letter in the name of the customer wrongly would not spoil system or lead to any loss, whereas, a financial data item may have serious repercussions. In some of the financial data input, two sets of record by different operators may be prepared and compared by the computer for any discrepancies. Regarding transaction fields and the permanent fields in the master file, there have to be different standards. An error in the transaction file, for example, punching 32 hours but by an operator in place of 23 hours he actually puts in, normally leads to one time error only and is unlikely to be repeated again. But an error in the master file, for example, rupees 11 per hour wage read against correct one of rupees 10 per hour is a perpetual source of error.

c. File Interrogation:
The purpose of file interrogation is to ensure that the correct file is being processed by the system. These controls are particularly important for master files, which contain permanent records of the firm and which, if destroyed or corrupted, are difficult to replace.

Internal label checks: These verify that the file processed is the one the program is actually calling for. Files stored on magnetic tape are usually kept off-line in a tape library. These files have an external label that identifies them (by name and serial number) to the tape librarian and the operators. External labeling is typically a manual procedure and, like any manual task, prone to errors. The wrong external label may be mistakenly affixed to a file when it is created. Thus, when the file is called for again, the wrong file will be retrieved and placed on the tape drive for processing. Depending on how the file is being used this may result in its destruction or

corruption. To prevent this, the operating system creates an internal header label that is placed at the beginning of the file.

To ensure that the correct file is about to be processed, the system matches the file name and serial number in the header label with the program's file requirements. If the wrong file has been loaded, the system will send a message to the operator and suspend processing. It is worth nothing that while label checking is generally a standard feature, it is an option that can be overridden by programmers and operators.

Version checks: These are used to verify that the version of the file being processed is correct. In a grandfather-father-son (GFS) approach, many versions of master files and transactions may exist. The version check compares the version number of the files being processed with the program's requirements.

An expiration date check prevents a file from being deleted before it expires. In a GFS system, for example, once an adequate number of backup files is created, the oldest backup file is scratched (erased from the disk or tape) to provide space for new files.

To protect against destroying an active file by mistake, the system first checks the retention period contained in the header label. If the retention period has not yet expired, the system will generate an error message and abort the scratch procedure. It is an optional measure and if the programmer chooses not to specify the retention period, the control against such accidental deletion is eliminated.

Input error correction: When errors are detected in a batch, they must be corrected and the records should be resubmitted for reprocessing. This must be a controlled process to ensure that errors are dealt with completely and correctly. There are three common error-handling techniques: 1. immediate correction, 2. Create an error file, and 3. reject the entire batch.

Immediate correction: if the system is using the direct data validation approach, error detection and correction can also take place during data entry. Upon detecting a key stroke error or an illogical relationship, the system should halt the data entry procedure until the user corrects the error.

Create an Error File: When delayed validation is being used, such as in batch systems with sequential files, individual errors should be flagged to prevent them from being processed. At the end of the validation procedure, the records flagged as errors are removed from the batch and placed in a temporary error holding file until the errors can be investigated.

Reject the Batch: Some forms of errors are associated with the entire batch and are not clearly attributable to individual records. An example of this type of error is an imbalance in a batch control total. Assume that the transmittal sheet for a batch of sales orders shows a total sales value of Rs. 121, 674, 87, but the input procedure calculated a sales total of only Rs. 121, 454.32. What has caused this? Is there problem of a missing or changed record? Or was the batch control total incorrectly calculated by the data control clerk? The most effective solution in this case is to cease processing and return the entire batch to data control to evaluate, correct, and resubmit.

PROCESSING CONTROLS

After passing through the data input stage, transactions enter the processing stage of the system. Processing controls are divided into three categories: run-to-run controls, operator intervention controls, and audit trail controls.

Run-to-Run Controls: The preparation of batch control figures was previously discussed as an element of input control. Run-to-run controls use batch figures to monitor the batch as it moves from one programmed procedure to another. These controls ensure that each run in the system processes

the batch correctly and completely. Batch control figures may be contained in either a separate control record created at the data input stage or an internal label. Specific uses of run-to-run control figures are described below.

Recalculate Control Totals: After each major operation in the process and after each run, amount fields, hash totals, and record counts are accumulated and compared to the corresponding values stored in the control record. If a record in the batch is lost, goes unprocessed, or is processed more than once, this will be revealed by the discrepancies between these figures.

Transaction Codes: The transaction code of each record in the batch is compared to the transaction code contained in the control record. This ensures that only the correct types of transaction is being processed.

Sequence Checks: In systems that use sequential master files, the order of the transaction records in the batch is critical to correct and complete processing. As the batch moves through the process, it must be re-stored in the order of the master file used in each run. The sequence check control compares the sequence of each record in the batch with the previous record to ensure that proper sorting took place.

Operator intervention controls: Systems sometimes require operate intervention to initiate certain actions, such as entering control totals for a batch of records, providing parameter values for logical operations, and activating a program from a different point when reentering semi-processed error records.

Operator intervention increases the potential for human error. Systems that limit operator intervention through operator's intervention controls are thus less prone to processing errors. Although it may be impossible to eliminate operator involvement completely. Parameter values and program start points should, to the extent possible, be derived logically or provided to the system through look-up tables.

Audit Trail Controls: The preservation of an audit trail is an important objective of process control. In an accounting system, every transaction must be traceable through each stage of processing from its economic source to its presentation in financial statements. In a computer based information systems (CBIS) environment, the audit trail can become fragmented and difficult to follow. It thus becomes critical that each major operation applied to a transaction be thoroughly documented. The following are examples of techniques used to preserve audit trails in a CBIS.

Transaction Logs: Every transaction successfully processed by the system should be recorded on a transaction log, which serves as a journal.

Transaction Listings: The system should produce a (hard-copy) transaction listing of all successful transactions. These listings should go to the appropriate users to facilitate reconciliation with input.

*Log of Automatic Transactions: S*ome transactions are triggered internally by the system. An example of this is when inventory drops below a preset reorder point, and the system automatically processes a purchase order. To maintain an audit trail of these activities, all internally generated transactions must be placed in a transaction log.

Listing of Automatic Transactions: To maintain control over automatic transactions processed by the system, the responsible end user should receivable a detailed listing of all internally generated transactions.

Unique Transaction Identifiers: Each transaction processed by the system must be uniquely identified with a transaction number. This is the only practical means of tracing a particular transaction through a database of thousands or even millions of records. In system that use physical source documents, the unique number printed on the document can be transcribed during data input and used for this purpose. In real-time systems, which do not use source documents, each transaction should be assigned a unique number by the system.

Error Listing: A listing of all error records should go to the appropriate user to support error correction and resubmission.

OUTPUT CONTROLS

Output controls ensure that system output is not lost, misdirected, or corrupted and that privacy is not violated. Exposures of this sort can cause serious disruptions to operations and may result in financial losses to a firm. For example, if the cheques produced by a firm's cash disbursements system are lost, misdirected, or destroyed, trade accounts and other bills may go unpaid. This could damage the firm's credit rating and result in lost discounts, interest, or penalty charges. If the privacy of certain types of output is violated, a firm could have its business objectives compromised, or it could even become legally exposed. Examples of privacy exposures include the disclosure of trade secrets, patents pending, marketing research results, and patient medical records.

The choice of controls employed to protect system output is influenced by the type of processing method in use. Generally, batch systems are more susceptible to exposure and require a greater degree of control than real-time systems. This section examines output exposures and controls for both methods.

Controlling batch system output: Once the data has been processed internally by the CPU, it is usually transferred to some form of output medium for storage, or in the case of printed output, prepared as a report for distribution and managerial use. Output controls involve this aspect of the data processing function. The two output controls we shall discuss here: (1) Tape and disk output controls, and (2) printed output controls

1. Tape and Disk output Controls: Computer output to magnetic tapes and disks is not normally verified by direct human observation as is the case with manually printed output. Hence, special care must be taken to ensure accuracy in encoding of information on these output media. Hardware controls such as parity bit checking, and software controls such as check digits can be carried out along with the informational output transmission to make sure that no digits are lost in the communication process.

   It may be noted that the disk drives and tape drives have built-in dual recording mode to enable these machines to check on recording accuracy. It works as follows:

   The disk/tape is encoded with the desired information, this information is read again using the reading mechanism of the tape or disk drive. A comparison is made to verify the original output. In most cases, the comparison of the initial output data with the newly recorded data will result in a confirmation of identical information, and the tape or disk system is then able to signal the CPU that the required writing operation has been successful. This is called the ECHO check. An unfavorable comparison implies that a hardware failure has occurred. In such instances, either a second writer attempt can be initiated, or computer operator notifies for alternative action.

   Use of file labels can be treated as an output control in case of tape and disk files. The file label processing requires the updating of information in trailer record to reflect the new status of the file. For example, the number of logical and physical records residing in the updated file must be recorded in trailer record since this information will be used as a processing controls when the file is later used for input.

Similarly, the file retention date should be carefully checked by the computer program and updated to indicate a longer retention cycle if it is deemed necessary.

The output control totals may also be incorporated for various applications. Examples can include the recording the rupee balances in an accounts payable file, the recording of hash totals for an inventory parts file and the recording of items summaries in a transaction file of credit-customer activity.

2. Output controls for printed output: the main requirements and techniques of output controls for printed output may be considered under the headings:

   a. verification of output;
   b. distribution of output;

It is important that the computer should be programmed to write page numbers, descriptive captions and processing dates on all print-outs.

Verification of output: The verification controls applied to output will be governed largely by the relationship which the output bears to the input and the processing that created it. Output may be considered in these terms under three headings:

i. output directly related to input;
j. output indirectly related to input;
k. exception reports

i. Output directly related to input: This would include;

- output that is identical with input, which usually results from updating or creating a file and takes the form of lists or documents (e,g., lists of master file amendments or purchase invoices, dispatch notes and cheques);
- output that is in part identical with input but includes additional information usually involving standing data (e.g., sales invoices produced from dispatch notes and prices, payrolls produced from clock cards and rates of pay)

  In these cases it is normal for the output to be verified clerically with thet controls established either before or during processing e.g., by agreeing control totals or checking output individually with retained copies of input documents).

j. Output indirectly related to input: this would include output generated by the programs on the basis of:

- current input data (e.g., reports of unmatched and missing items);
- previous or latest input data (e.g., overdue debtor reminder procedures);
- all input for a given period (e.g., personal and nominal ledgers, interest charges and cumulative totals).

  While output of this nature is often verified clerically with the cumulative controls established over the relevant input (e.g., a debtor's controls account), more reliance is usually place don the correct functioning of the computer programs than is normally the case with output directly related to input data.

k. exception reports: These would include reports of items identified by the computer programs from a security of input data or master file as not satisfying conditions specified in the program (e.g., net pay in excess of a specified amount, or slow moving stock). It is not normally practicable to verify

exception reports clerically with the controls established over input or master files. Their complete and accurate production almost always depends on the correct functioning of the computer programs.

Distribution of output: If the user department that verifies the controls also acts on the output it will be apparent to the user department whether it received all that output. If, however, the verification is carried out in the computer department or the output is not verified with the controls established over input or master file (e.g., exception reports) procedures are required to ensure that the user department responsible receives all output intact. These procedures often take the form of output registers or the sequential numbering of exception reports.

Procedures for acting on exception reports: Exception reports often provide the information on which important control functions are based (e.g., controls of overtime). A high degree of control is thus usually required over the investigation of exception reports and the resulting action taken. This will often take the form of an independent review of exception reports to ensure that the exceptional items are promptly investigated and acted upon.

Controlling real-time systems output: Real-time systems direct their output to the user's computer screen terminal, or printer. This method of distribution eliminates the various intermediaries in the journey from the computer center to the user and thus reduces many of the exposures discussed above. The primary output threat to real-time output is the interception, disruption, destruction, or corruption of the output message as it passes along the communications link. This threat comes from two types of exposures:

1. exposures from equipment failure and
2. exposures from subversive acts, whereby a computer criminal intercepts the output message transmitted between the sender and the receiver. Techniques for controlling communications exposures were discussed previously.

CHAPTER 15

DETECTION OF COMPUTER FRAUDS

COMPUTER FRAUDS

Computer frauds have been defined as any illegal act for which knowledge of computer technology is essential for its perpetration, investigation or prosecution. Most specifically, computer frauds include the following:

- unauthorized theft, use, access, modification, copying and destruction of software or data
- theft of money by altering computer records or the theft of computer time
- theft or destruction of computer hardware
- use of a plan to operate computer resources to commit an offence
- intend to illegally obtain information or tangible property through the use of computer

using the computer, fraud perpetrators are able to steal more, in much less time and with much less efforts. For example, they can steal millions of rupees in less than a second. Perpetrators can commit a fraud and leave little or no evidence. Therefore, computer fraud is often much more difficult to detect than other types of frauds.

It might be generally thought that computer fraud means no more than "using a computer to commit fraud". This is far too narrow definition in view of the many ways that businesses can face the risk of loss as a result of the use or misuse of a computer.

A more extensive definition of computer fraud could be as given below:
"Using a computer to cause prejudice, in the sense of financial and/or reputational damage, to a business" may be called a computer fraud.

The definition of computer fraud would include (but not be limited to) the following:

a. *Clearly recognizable frauds* such as investment frauds, secret market frauds and pyramid schemes where a computer (usually via the Internet) is used as a new medium to convey an old message and the helpless victim is persuaded to participate with money or credit card details. Most of the frauds that are prevalent on the Internet frauds are a variation on this theme. Victims are influenced that there is a confidential and exclusive market for a particular kind of financial instrument a "prime bank guarantee" which offers a high rate of return. Pyramid schemes again offer high returns for small contribution and invariably collapse leaving the last to join without prospect of recovering any funds.
b. *Hacking* in the generally recognized sense, unauthorized access and unauthorized modification to computers. This includes the malicious introduction of a virus, the malicious modification of email or the vandalism of Web pages. This is now a popular activity among hackers and considered to be real problem for anyone doing business on the Internet.
c. *Manipulation of computer systems to obtain money from an employer or a third party*. Examples of this are diversion of payments and creation of false employees/suppliers. These frauds may require access to a system or part of a system. As we know that businesses often fail to implement even the most basic password and access controls. They thus allow access to their systems, which could easily be denied.
d. *Theft and/or destruction of confidential and sensitive information*. This is an area where huge damage can be caused by employees and third parties who are able to gain access to confidential and sensitive information and pass it on to competitors or simply destroy it;
e. *Abuse of computer systems by employees.* This involves an employee using the computer system for his or her own purposes. Employees can write personal letter or run businesses from their employer's computers. Employees can use email systems and the Internet for private purposes.
f. *Software piracy* by either using counterfeit or unlicensed software or by distributing counterfeit software by disk, CD or through the Internet.

WHY SHOULD BUSINESSES TAKE COMPUTER FRAUD SERIOUSLY?

All businesses need to assess the adequacy of their protection against computer fraud, even those that do not currently do business on the Internet, since

a. all businesses are now dependent on ne+tworked or stand alone computers;
b. individual businesses are increasingly linked through computer networks or by electronic payment systems;
c. the growth of electronic commerce means more businesses connected to the Internet and more risk of hacking;
d. the predicted growth of electronic cash means a real risk of interception, theft or destruction of electronic payments during transmission;

It may be stated that computer fraud is very different from conventional fraud in a number of important respects:

1. It is easily hidden and hard to detect. Unlike conventional frauds, there may be no easily recognisable audit trail and the fraud is likely to be hidden in enormous volumes of data.
2. Evidence of computer crime may be not only hard to find, but also difficult to present to a court in away which is effective or legally admissible.
3. It is easily committed in ways that may not be obvious:

   - it involves the manipulation of "invisible" data;
   - a few key strokes are all that may be needed;
   - a business's computer can be remotely accessed, both by employees and outsiders;
   - huge amounts of data can be transported on a single floppy disk which can be written to in a matter of seconds.

Whilst this is not universally true, there is still a general lack of knowledge about how computer work and how systems can be protected which enables fraudsters to take advantage. The damage caused by interference with computer systems can be out of all proportion to the effort required to cause the damage. For example, the insertion of a virus may take a matter of minutes but wipe out all the data that the business has collected from its commencement.

WHAT ARE THE PRIMARY RISKS TO BUSINESS?

Let us now look at the risks to business from computer fraud in terms of internal threats. That is to say from the business' own staff and external threats, intrusions by outsiders. Possibly working in collusion with staff.

Internal threats: There is evidence that internal fraud is a greater risk to business than external fraud. A survey carried out in May 1996 found that four out of five of the most serious frauds involved employees. One in five frauds involved collusion between an employee and outsider.

One way to categorize computer internal fraud is to use the data processing model: input, processing computer instructions, stored data and output.

1. **Input**: The simplest and most common way to commit a fraud is to alter computer input, it requires little, if any, computer skills. Instead, perpetrator needs only to understand how the system operates so that they can cover their tracks.

   In collusive fraud, one perpetrator opens an account at a bank, and then prepared blank deposit slip. The slips were similar to those available in bank lobby, except that his account number was encoded on them. One morning he replaced all the deposit slips in the bank lobby with his forged ones. For three days all bank deposits using the forged slips went directly into his account. After three days the perpetrator withdrew the money and disappeared. He used alias: his identity was never uncovered nor was he ever found.

In disbursement frauds, the perpetrator causes a company either pay too much for ordered goods or to pay goods that were never ordered. One perpetrator used a DTP package to prepare fraudulent bills for office supplies that were never ordered, then mailed those bills to companies across the country. The perpetrator kept the amount low enough so that most companies did not bother to require purchase orders to approvals. An amazingly high percentage of the companies paid the bills without question.

To commit *payroll frauds*, perpetrators can enter data to increase the salary, create a fictitious employee, or retain a terminated employee on the records. Under the latter two approaches, the perpetrator proceeds to intercept and cash the illegal cheques.

In a *cash receipts fraud*, the perpetrator hides the theft by falsifying system input. For example, an employee at the Arizona Veteran's Memorial Coliseum sold customers full price tickets, entered the sales as half-price tickets, and pocketed the difference.

2. **Process:** Computer fraud can be committed through unauthorized system use. Including the theft of computer time and services. For example, some companies do not permit employees to use company computers to keep personal or outside business records. Violating this policy would constitute a fraud. While most people would not call it fraud employee goofing (surfing the Internet for personal entertainment on company time) has become a serious problem at many companies. One study estimates that employees with access to the Internet, on average, lose one to two hours of productivity a week goofing.

3. **Computer Instructions:** Computer fraud can be accomplished by tampering with the software that processes company data. This may involve modifying the software, making illegal copies, or using it in an unauthorized manner. It might also involve developing a software program or module to carry out an unauthorized activity. This approach to computer fraud used to be one of the least common, because it requires a specialised knowledge about computer programming that is beyond the scope of most users. Today, however, such frauds are much more frequent because there are many web pages with instructions on how to create viruses and other computer instruction based schemes.

4. **Data:** Computer fraud can be perpetrated by altering or damaging a company's data files or by copying, using, or searching them without authorization. There have been numerous instances of data files being scrambled, altered, or destroyed by disgruntled employees. In one instance, an employee removed all the external labels from hundreds of tape files. In another case, an employee used a powerful magnet to scramble all the data on magnetic files.

   Company data can also be stolen. In one case, the office manager of a Wall Street law firm found information about prospective mergers and acquisitions in the firm's word processing files. He sold the information to friends and relatives, who made several millions dollars by illegally trading securities.

   Data can be destroyed, changed, or defaced-particularly if stored on a computer web site. One noted hacker stated that all companies that use the web, especially those with important trade secrets or valuable information technology assets, are under constant attack.

5. **Output**: Computer fraud can be carried out by stealing or misusing system output. System output is usually displayed on monitors or printed on paper. Unless properly safeguarded, monitor and printer output is subject to pry eyes and unauthorized copying.

External threats: The dangers of hacking are well known. The main threats from hacking are:

- Removal of information;
- Destruction of system integrity:
- Interference with web pages;
- Transmission of viruses by email.
- Interception of email
- Interception of electronic payments

INTERNET FRAUDS

Another major external threat is fraud perpetrated over the Internet. Just as the Internet can and should be used for legitimate commerce, so can its power be harnessed for criminal and fraudulent purposes. There are a number of characteristics of the Internet, which are likely to attract fraudsters seeking to make easy money from innocent victims:

- It is unregulated in so far as who may set up a site. No license fees are payable to any central authority and no form of inspection is, or in practical terms ever could be carried out on those persons or entities setting up sites.
- An Internet site can be set up anywhere in the world at very low cost and can reach anywhere else in the world at low cost. This means that fraudsters now have "global reach" and can access a far larger market of potential victims than ever before. As fraudsters are always looking for new victims, this is a very attractive feature.
- An impressive site with links to established companies or financial institutions may be no more than an empty shell designed to attractive and trap the unwary. There is no easy way of separating the genuine from the false.
- The glamour and novelty of the Internet and the spurious credibility claimed by a site may cause otherwise prudent investors to become involved in fraudulent schemes.
- A site may, and probably will, operate outside the legal jurisdiction of the country in which the victim of the fraud resides. A company which gives itself a UK Internet address need have absolutely no legal or commercial connection with the jurisdiction.

The above factors make it extremely difficult to discover, in sufficient time to effect recovery or at all, the identity of the www site operator.

THE RISE IN COMPUTER FRAUDS

Organizations that track computer fraud estimate that 80% of businesses have been victimized by at least one incident of computer fraud. However, for the following reasons no one knows for sure exactly how many companies loose to computer fraud.

1. Not everyone agrees on what constitute computer fraud. For example, some people restrict the definition to a crime that takes place inside a computer or is directed at it. For others it is any crime where the perpetrator uses the computer as a tool. Many people do not believe that making an unlicensed copy of software constitute computer fraud. Software publishers however, think otherwise.
2. Many computer frauds go undetected. It is estimated that only 1% of all computer crime is detected.
3. 80-90% of the frauds data that are uncovered are not reported. Only the banking industry is required by law to report all frauds. The most common reason for failure to report computer fraud is a company's fear that adverse publicity would result in fraud and loss of customer confidence that would cost more than the fraud itself.
4. Most networks have a low level of security, it is estimated that two out of three sides have serious vulnerabilities, and most firewalls and other protective measures at the sites are ineffective.
5. Many Internet pages give step by step instructions on how to perpetrate computer frauds and abuses. There are also thousands of pages on how to break into routers and disable web servers.
6. Law enforcement is unable to keep up with the growing number of computer frauds.

Frauds on the Internet proliferate: The following are a few examples collected in recent months from the press.

1. The officers of a small Illinois company created the Agency for Inter-American Finance on the WWW in the late 1995. The WWW site hosted with impressive graphics and was linked to the Internet by a Swiss Internet Service provider. AIF claimed to be based in Antigua and that it was a provider of investment capital for Latin American businesses. A three year tax free "Inter American Hard Currency Bond" at a cost of US$ 2,500 with a guaranteed rate of return of 11.75% per year. It was claimed that American Pacific Financing Ltd., guaranteed the bonds. The site was linked to a number of established financial service businesses and the impression given that it was genuine and well placed. In fact, an investigation revealed that AIF was a Panamanian shell company, and that the bond and guarantor were fake. The identity of the perpetrators was not discovered. This fraud exemplifies the factors peculiar to Internet frauds, described above.
2. In 1997 the US Federal Trade Commission began litigation against a company called "Fortuna Alliance" which had an Internet site. This company offered investors a return of $5,000 per month for an investment of $250. It might be thought that no one would be foolish enough to invest in such an improbable scheme but in fact investors lost about $6 million before the FTC blocked access to the site.
3. In August 1997, the European Union Bank which, traded over the Internet, collapsed. It was registered in Antigua and had been founded by two Russians in 1994. The site claimed that it offered a $1 million certificate of deposit that paid interest of 9.91%. It had attracted unfavorable comment by the Bank of England sometime before it collapsed.
4. Offshore trusts are mainly an American problem. Internet sites and bulk email schemes promise freedom from US taxes if victims transfer their assets to an offshore trust and pay a handsome fee. What happens is that the fraudsters either decamp with the fees (often thousands of dollars) or set up the trusts and make themselves beneficiaries, thus all the victims' assets held with them.

COMPUTER FRAUD AND ABUSE TECHNIQUES

Some of the techniques are briefly discussed below:

Technique	Description
Cracking	Unauthorized access to and use of computer systems, usually by means of a personal computer and a telecommunications network. Crackers are hackers with malicious intentions.
Data Diddling	Changing data before, during, or after it is entered into the system in order to delete, alter, or add key system data.
Data leakage	Unauthorized copying of company data such as computer files.
Denial of service attack	Attacker sends e-mail bombs (hundreds of messages per second) from randomly generated false addresses; Internet service provider's e-mail is overloaded and shuts down.
Eavesdropping	Listening to private voice or data transmissions, often using a wiretap.
E-mail forgery	Sending an e-mail message that looks as if it were sent by someone else.
E-mail threats	Sending a threatening messages to try and get recipient to do something that would make it possible to defraud him
Hacking	Unauthorized access to and use of computer systems, usually by means of a personal computer and a telecommunications network. Hackers do not intend to cause any damage.
Internet misinformation	Using the Internet to spread false or misleading information about companies
Logic time bomb	Program that lies idle until some specified circumstance or a particular time triggers it. Once triggered, the tomb sabotages the systems by destroying programs, data, or both
Masquerading or impersonation	Perpetrator gains access to the system by pretending to be an authorised user. Enjoys same privileges as the legitimate user.

Password cracking	Intruder penetrates a system's defenses, steals the file containing valid passwords, decrypts them, and then uses them to gain access to system resources such as programs, files, and data.
Piggybacking	Tapping into a telecommunications line and latching on to a legitimate user before he logs into the system: legitimate user unknowingly carries perpetrator into the system
Round-down	Computer rounds down all interest calculations to two decimal places Remaining fraction of a cent is placed in an account controlled by perpetrator.
Salami technique	Tiny slices of money are stolen over a period of time (Expenses are increased by a fraction of a percent: increments are placed in a dummy account and later pocketed by the perpetrator).
Scavenging	Gaining access to confidential information by searching corporate records. Scavenging methods range from searching trashcans for printouts or carbon copies of confidential information to scanning the contents of computer memory.
Social engineering	Perpetrator tricks an employee into giving out the information needed to get into a system.
Software piracy	Copying computer software without the publisher's permission.
Spamming	E-mailing the same message to everyone on one or more Usenet news groups or LISTSERV lists.
Super zapping	Unauthorized use of special system programs to bypass regular system controls and perform illegal acts.
Trap door	Perpetrator enters the system using a back door that bypasses normal system controls and perpetrates fraud.
Trojan horse	Unauthorized computer instructions in an authorized and properly functioning program.
Virus	Segment of executable code that attaches itself to software, replicates itself, and spreads to other systems or files. Triggered by a predefined event, a virus damages system resources or displays a message on the monitor.
War dialing	Programming a computer search for an idle modem by dialing thousands of phone lines. Perpetrator enters the system through the idle modem. Captures the personal computer attached to the modem, and gains access to the network to which the personal computer is attached.
Worm	Similar to a virus, except that it is a program rather than a code segment hidden in a host program. A worm also copies and actively transmits itself directly to other systems. It usually does not live very long, but it is quite destructive while it is alive.

PREVENTING COMPUTER FRAUDS

Because fraud is such a serious problem, organizations must take every precaution to protect their information systems. A number of measures can significantly decrease the potential for fraud and any resulting losses.

a. *Make Fraud less Likely to Occur:* Some computer consultants claim that the most effective method of obtaining adequate system security is to rely on the integrity of company employees. At the same time, research shows that most frauds are committed by current and former employees. Thus employees are both the greatest control strength and weakness. Organizations can take steps to increase employee integrity and reduce the likelihood of employees committing a fraud.
b. *Use Proper Hiring and Firing Practices:* A manger's most important responsibility is to hire and retain honest people. Similarly, a company should be very careful when firing employees. Dismissed employees should be removed from sensitive jobs immediately and denied access to the computer system to prevent damage or copying confidential data before they leave.

c. *Manage Disgruntled Employees:* Many employees who commit fraud are seeking revenge or "justice" for some wrong they perceive has been done to them. Hence companies should have procedures for identifying these individuals and either helping them resolve their feelings or removing them from jobs with system access.
d. *Train Employees in Security and Fraud Prevention Measures:* Many top executives believe that employee training and education is the most important element of any security program. Fraud is much less likely to occur in an environment where employees believe security is everyone's business.

To develop this type of culture, a company should educate and train employees in the following areas:

1. **Security measures:** Employees should be well-schooled in security measures, taught why they are important, and motivated to take them every seriously.
2. **Telephone disclosures:** Employees should be taught to not give out confidential information over the telephone without knowing for sure who is calling. The employees can be taught tactics such as dialing the caller back and verifying a person's identity by asking specific questions that only they would be able to answer.
3. **Fraud awareness:** Employees should be made aware of fraud, its prevalence, and its dangers. They should be taught why people commit fraud and how to deter and detect it.
4. **Ethical considerations:** The company should promote its ethical standards in its practices and through company literature such as employee handouts. Acceptable and unacceptable behavior should be defined so that employees are aware of a company's ethical position. Many business practices fall into a gray area between right and wrong, and this problem is especially prevalent through out the computer industry. For example, many professions see nothing wrong with utilizing corporate computer resources for personal use or gaining unauthorized access to another company's databases and browsing through them. One programmer, when arrested for unauthorized browsing, was shocked that he was prosecuted for his crime; he felt that his activities were a common industry practice.
5. **Punishment for unethical behavior:** Employees should be informed of the consequences of unethical behavior (scolding, dismissal, prosecution, etc.) This information should be disseminated not as a threat but as the consequence of choosing to act unethically. For example, employees should be informed that using a computer to steal or commit fraud is a federal crime and anyone so doing faces immediate dismissal and/or prosecution. Likewise, the company should display notices of program and data ownership and inform employees of the penalties of misuse.
6. **Educating employees** in security issues, fraud awareness, ethical considerations, and the consequences of choosing to act unethically can make a tremendous difference.
7. **Manage and Track Software Licenses:** Software license management, a fast growing area of information technology management, helps companies make sure they comply with all their software licenses. Of key concern is making sure there are enough licenses to met user demands and that there are not more users than licenses. This protects them from software piracy lawsuits. It can also save the company money ensuring that it does not pay for more licenses than they actually use or need.
8. **Require Signed Confidentiality Agreements:** All employees vendors, and contractors should be required to sign and abide by a confidentiality agreement.

INCREASE THE DIFFICULTY OF COMMITTING FRAUD

One way to deter fraud is to design a system with sufficient controls to make fraud difficult to perpetrate. These controls help ensure the accuracy, integrity, and safety of system resources.

1. *Develop a Strong System of Internal Controls:* The overall responsibility for a secure and adequately controlled system lies with top management. Managers typically delegate the design of adequate control systems to systems analysts, designers, and end users. The corporate

information security officer and the operations staff are typically responsible for ensuring that control procedures are followed.

It is especially important to make sure that internal controls are in place during the end-of-the-year holiday season. Research shows that a disproportionate amount of computer fraud and security break-ins takes place during the holidays.

2. *Segregate Duties:* As discussed earlier, there must be an adequate segregation of duties to prevent individuals from stealing assets and covering up their tracks.
3. *Require Vacations and Rotate Duties:* Many fraud schemes, such as lapping and kiting, require the ongoing attention of the perpetrator. If mandatory vacations were coupled with a temporary rotation of duties, such ongoing fraud schemes would fall part.
4. *Restrict access to Computer Equipment and Data Files:* Computer fraud can be reduced significantly if access to computer equipment and data files is restricted. Physical access to computer equipment should be restricted, and legitimate users should be authenticated before they are allowed to use the system. Unfortunately, companies often fail to delete or change ID codes and passwords when employees leave or are transferred to another department.
5. *Encrypt Data and Programs:* Another way to protect data is to translate it into a secret code, thereby making it meaningless to anyone without the means to decipher it.
6. *Protect Telephone Lines:* Computer hackers use telephone lines to transmit viruses and to access, steal, and destroy data.
   One effective method to protect telephone lines is to attach an electronic lock and key to them.
7. Protect the System from Viruses: There are hundreds of thousands of virus attacks every year, and an estimated 90% of the PCs that suffer a virus attack are reinfected within 30 days by the same virus or some other virus. A system can be protected from viruses using virus protection software.

   Fortunately, some very good virus protection programs are available. Virus protection programs are designed to remain in computer memory and search for viruses trying to infiltrate the system. The intrusion is usually detected when there is an unauthorized attempt to access an executable program. When an infection attempt is detected, the software freezes the system and flashes a message to the user. The user can then instruct the program to remove the virus. Virus detection programs, which spot an infection soon after it starts, are more reliable than virus protection programs. Virus identification programs scan all executable programs to find and remove all known viruses from the system. These programs work by scanning the system for specific characteristics of known virus strains.

   Make sure that the latest versions of the anti-virus programs are used.

8. *Control Sensitive Data:* To protect its sensitive data, a company should classify all of its data as to importance and confidentiality and then apply and enforce appropriate access restrictions. Controls can be placed over data files to prevent or discourage copying. Employees should be informed of the consequences of using illegal copies of software, and the company should institute controls to see that illegal copies are not in use. Sensitive and confidential information, backup tapes, and system documentation should be locked up at night and should not be left out on desks. Servers and PCs should also be locked when not in use. Companies should never store all of their data in one place or give an employee access to all of it. Local area networks can use dedicated servers that allow data to be downloaded but never uploaded to avoid infection by a network computer. Closed-circuit televisions can be used to monitor areas where sensitive data or easily stolen assets are handled.
9. *Control Laptop computers:* Special care should be given to laptops because thieves are increasingly breaking into cars and hotel rooms to steal laptops for the confidential information they contain. To control laptops, companies should take following measures:

- Establish laptop security policies to require employees to back up data before travelling and to a separate source when on the road, and to never leave a laptop unattended.
- Install software that makes it impossible for the computer to boot up without a password.
- Password protect and encrypt data on the hard disk so that if a laptop is stolen, the data can not be used.
- Employees should be asked to store confidential data on a disk, rather than the hard drive, and always keep the diskette in their possession.

IMPROVE DETECTION METHODS

Many companies are currently being defrauded and do not know it. The following steps can be taken to detect fraud as soon as possible.

1. *Conduct Frequent Audits:* One way to increase the likelihood of detecting fraud and computer abuses is to conduct periodic external and internal audits as well as special network security audits. Auditors should regularly test system controls and periodically browse data files looking for suspicious activities. However, care must be exercised to make sure employees' privacy rights are not violated.
2. *Use a Computer Security Officer:* Most frauds are not detected by internal or external auditors. The study shows that assigning responsibility for fraud deterrence and detection to a computer security officer has a significant deterrent effect. This person should be independent of the information system function. The security officer can monitor the system and disseminate information about improper system uses and their consequences.
3. *Use Computer Consultants:* Many companies use outside computer consultants or in house teams to test and evaluate their security procedures and that is detected is closely evaluated, and corresponding protective measures are implemented. Some companies dislike this approach, because neither they want their weaknesses to be exposed nor do they want their employees to know that the system can indeed be broken into.
4. *Monitor system Activities:* All system transactions and activities should be recorded in a log. The log should indicate who accessed what data, when, and from which terminal. These logs should be reviewed frequently to monitor system activity and trace any problems to their source.

   There are a number of risk analysis and management software packages that can review computer systems and networks. These systems evaluate security measures already in place and test for weakness and vulnerabilities. A series of reports is then generated that explain the weaknesses found and suggest improvements.

5. *Use Fraud Detection Software:* People who commit fraud tend to follow certain patterns and leave behind telltale clues, such as things that do not make sense. Software has been developed to search out these fraud symptoms.

REDUCE FRAUD LOSSES

No matter how hard a company tries to prevent fraud, chances are that it will occur. Therefore, an important strategy is to seek to minimize potential fraud losses. Some of these methods include the following:

- Maintain adequate insurance.
- Keep a current backup copy of all program and data files in a secure off-site location.
- Develop a contingency plan for fraud occurrences and other disasters that might occur.
- Use special software designed to monitor system activity and help companies recover from frauds and malicious actions.

PROSECUTE AND INCARCERATE FRAUD PERPETRATORS

Most fraud cases go unreported and unprosecuted for several reasons.

First, many cases of computer frauds are as yet undetected.

Second, companies are reluctant to report computer crimes because a highly visible computer fraud is a public relations disaster. Fraud also reveals the vulnerability of its system, possibly attracting more acts of fraud. Unreported fraud creates a false sense of security; people think systems are more secure than they really are.

Third, law enforcement officials and the courts are so busy with violent crimes that they have little for fraud cases where no physical harm is present.

A fourth reason fraud goes unreported is that it is difficult, costly, and time-consuming to investigate.

A fifth reason for unreported fraud is that many law enforcement officials, lawyers, and judges lack the computer skills needed to investigate, prosecute, and evaluate computer crimes. Increased training, which is time-consuming and costly, is necessary in order for officials to understand and detect computer fraud.

Finally, when fraud cases are prosecuted and a conviction is obtained, the sentences received are often very light. One investigator noted that the average sentence for a fraud perpetrator was one year in jail for every Rs. 10 million stolen.

DETECTION OF COMPUTER FRAUDS

To reduce the risk to business from computer fraud, computer forensic tools can be used. These have a much wider application than just dealing with computer fraud. They can be applied in any investigation where every computer may hold relevant evidence.

We would focus in this chapter on just one of these tools viz., disk imaging and analysis.

Disk imaging and analysis Technique: It enables the fraud investigator to discover evidence of transactions that the fraudster thought were inaccessible or had been destroyed. For example, such evidence may be in the form of word processing documents showing the stages in creation of a forged invoice or a blackmail letter; or files which demonstrate that an employee has been sending confidential information by e-mail to a competitor or copies of passwords of other members of staff or users of other computers or unclean material. The technique used for analyzing such evidence is discussed below:

The stages are as follows:

1. Using specialist hardware and software without the suspect necessarily being alerted, an exact copy of the computer hard disk is taken leaving the original completely intact and leaving no trace of the copying process. This is achieved by attaching the imaging hardware to the parallel port of the computer and running the imaging software without using the computer's operating system. This preserves the integrity of the hard disk and the confidentiality of the investigation. The image is written directly to an optical disk which can then be used for investigative purposes.
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. The recovery of deleted files seems like magic to the inexperienced. In fact, it is a relatively straightforward process and one that is important to understand if the full benefits of disk imaging and analysis are to be appreciated. When a file is created on a computer, a reference to it is stored in the computer's file allocation table. This may be compared with the contents page or index of a book. Under normal circumstances, when a file is deleted from within the operating system in which it was created, the actual bytes that contain the file information are not physically removed from the hard disk. All that happens is that the reference to the file in the file

allocation table is removed. This means that the space occupied by the file is made available to be overwritten by other data. However, at the time the image is taken it is probable that there will be a number of deleted files or file fragments that have not been overwritten and are therefore available to the investigator. The processing software can recover them.

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. The search is across all the text on the disk so that files which the suspect thinks have been destroyed and data which he may well have had no idea was being retained are searched. The extent of the searches depends upon the software used. In general terms, it should be possible to carry out single word searches, searches for phrases. Searches for numbers, searches for parts of words and phrases, searches for words which sound like other words and linked searches of more than one word or phrase using Boolean operators (and, or, if, not etc). Outside the normal file structure, that is to say where live files are usually stored, information can be recovered for investigation from:

   a. Free space—It refers to areas of a file system not currently allocated for data storage. These areas may have been used before and may contain deleted data. Which has not yet been overwritten.
   b. Lost chains—It refers to areas of the disk allocated for data storage but currently without a name or disconnected from the file system.
   c. Slack space—it refers to disk space allocated to files in allocation blocks normally of several hundred to several thousand bytes in size. Files rarely occupy a complete number of allocation blocks so some of the last allocation block will be unused. This area may contain data. Which has not been overwritten.
   d. Deleted files: Files that have been “undeleted” by the processing software and made available for interrogation.
   e. The contents of the Windows SWAP file—This is a disk cache by Windows each time it is run. It is a storage area in which all kinds of data may be kept. The file may be large and is hidden from the user. It is seldom deleted and can contain entire documents, memoranda and database information. It can thus be extremely valuable to an investigator.
   f. Internet cache files or temporary Internet files—When the Internet is accessed through Windows 95, copies of the Web pages looked at by the user are copied to the user’s computer. These copies are stored in a folder called Temporary Internet files. Again, this folder is seldom inspected by the user and the files are seldom deleted. They can be of great interest to the investigator as it might provide a route map of Internet access.

CHAPTER 16

CYBER LAWS AND INFORMATION TECHNOLGY ACT 2000

BRIEF HISOTRY

Need:

New communication system and digital technology have made dramatic changes in the way we live and the means to transact our daily business. There is a remarkable change in the way people transact business. Businessmen are increasingly using computers to create, transmit and store information in electronic form instead of traditional paper documents. It is cheaper, easier to store and retrieve and speedier to communicate. Although people are aware of the advantages which the electronic form of business provides, people are reluctant to conduct business in the electronic form due to lack of appropriate legal frame work. Electronic commerce eliminates need for paper based transactions. The two principle hurdles which stand in the way of facilitating electronic commerce and electronic governance, are the requirements of writing and signature for legal recognition. At present many legal provisions assume the existence of paper based records and documents which should bear signatures. The Law of Evidence is traditionally based upon paper-based records and oral testimony. Hence, to facilitate E-commerce, the need for legal changes has become an urgent necessity.

The Government of India realized the need for introducing a new law and for making suitable amendments to the existing laws to facilitate e-commerce and give legal recognition to electronic records and digital signatures. The legal recognition to electronic records and digital signatures in turn will facilitate the conclusion of contracts and the creation of legal rights and obligations through the electronic communication like Internet. This gave birth to the Information Technology Bill, 1999.

In May, 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000. This Act aims to provide the legal infrastructure for E-commerce in India and would have a major impact for E-businesses and the new economy in India. Therefore, it is important to understand what are the various perspectives of the IT Act, 2000 and what it offers.

OBJECTIVES OF THE ACT

The objectives of the Act are:

a. To grant legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication commonly referred to as “electronic commerce” in place of paper based methods communication
b. To give legal recognition to Digital Signature for authentication of any information or matter which requires authentication under any law;
c. To facilitate electronic filing of documents with Government departments.
d. To facilitate electronic storage of data;
e. To facilitate and give legal sanction to electronic fund transfers between banks and financial institutions.
f. To give legal recognition for keeping books of account by Bankers in electronic form.
g. To amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers’ Book Evidence Act, 1891 and the Reserve Bank of India act, 1934.

The detailed act is discussed below.

INFORMATION TECHNOLOGY ACT, 2000

SCOPE OF THE ACT AND DEFINITIONS (CHAPTER I)

This Act is called the Information Technology Act, 2000.

It shall extend to the whole of India and, unless otherwise provided in the Act, it applies also to any offence or contravention thereunder committed outside India by any person.

It shall come into force on such date as the Central Government may, by notification, appoint. Different dates may be appointed for different provisions of this Act.

It may be noted that the date from which the Act becomes effective is yet to be notified.

The Act shall not apply to following:

(a) a negotiable instrument as defined in section 13 of the Negotiable Instruments Act, 1881;
(b) a power-of-attorney as defined in section 1A of the powers-of-Attorney Act, 1882;
(c) a trust as defined in section 3 of the Indian Trusts Act, 1882;
(d) a will as defined in Section (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called;
(e) any contract for the sale or conveyance of immovable property or any interest in such property;
(f) Any such class of documents or transactions as may be notified by the Central Government in the Official Gazette.

Arrangement of sections: The Act consists of 94 sections spread over thirteen chapters, and four schedules to the Act. The various chapters are discussed in detail later. The Schedules to the Act contain related amendments made in other acts as outlined in the objectives of the Act, namely, the Indian Penal Code, the Indian Evidence Act, 1972, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India, 1934.

Definitions

Section 2 defines the various expressions occurring in the Act.

Some of the important terms are defined below:

a. "Access" with its grammatical variations and related expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;
b. "addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary'
c. "affixing digital signature" with its grammatical variations and related expression means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature;
d. "appropriate Government" means the Central Government except in some cases where it means the State Government:
e. "asymmetric crypto system" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;
f. "computer" means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory function by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;
g. "computer network" means the interconnection of one or more computers through
    1. the use of satellite, microwave, terrestrial line or other communication media; and
    2. terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained.
h. "computer resource" means computer, computer system, computer network, data, computer data base or software;
i. "computer system" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmers, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;
j. "data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

k. "digital signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;
l. "electronic form" with reference to information means any information generated sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;
m. "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;
n. "function", in relation to a computer, includes logic, control arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;
o. "information" includes data, text, images, sound, voice, codes, computer programs, software and databases or micro film or computer generated micro fiche:
p. "intermediary" with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message;
q. "key pair", means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;
r. "originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, st0ored or transmitted to any other person but does not include an intermediary;
s. "prescribed" means prescribed by rules made under this Act;
t. "private key" means the key of a key pair used to create a digital signature;
u. "public key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;
v. "secure system" means computer hardware, software, and procedure that
    1. are reasonably secure from unauthorized access and misuse;
    2. provide a reasonable level of reliability and correct operation;
    3. are reasonably suited to performing the intended functions; and
    4. adhere to generally accepted security procedures;
w. "verify" in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether
    1. the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;
    2. the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

AUTHENTICATION OF ELECTRONIC RECORDS USING DIGITAL SIGNATURES (CHAPTER II)

This section provides the conditions subject to which an electronic record may be authenticated by means of affixing digital signature. The digital signature is created in two distinct steps. First 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 the intended communication contained in the electronic record. Any tampering with the contents of the electronic record will immediately invalidate the digital signature. Secondly, 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 such private key. This will enable anybody to verify whether the electronic record is retained intact or has been tampered will since it was so fixed with the digital signature. It will also enable a person who has a public key to identify the originator of the message.

For the purpose of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally 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 its 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)

This chapter is of the most important chapters. It specifies the procedures to be followed for sending and receiving of electronic records and the time and the place of the dispatch and receipt. This chapter contains sections 4 to 10.

Section 4. This section provides for "legal recognition of electronic records". It provides that where any law requires that any information or matter should be in the typewritten or printed form then such requirement shall be deemed to be satisfied if it is in an electronic form.

Section 5. This section provides for legal recognition of Digital Signatures. Where any law requires that any information or matter should be authenticated by affixing the signature of any person, then such requirement shall be satisfied if it is authenticated by means of Digital Signatures affixed in such manner as may be prescribed by Central Government.

For the purposes of this section, "signed", with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" shall be construed accordingly.

Section 6 lays down the foundation of Electronic Governance. It provides that the filing of any form, application or other documents, creation, retention or preservation of records, issue or grant of any license or permit or receipt or payment in Government offices and its agencies may be done through the means of electronic form. The appropriate Government has the power of prescribe the manner and format of the electronic records and the method of payment of fee in that connection.

Section 7 This section provides that the documents, records or information which has to be retained for any specified period shall be deemed to have been retained if the same is retained in the electronic form provided the following conditions are satisfied:

1. The information therein remains accessible so as to be usable subsequently.
2. The electronic record is retained in its original format or in a format which accurately represents the information contained.
3. The details which will facilitate the identification of the origin, destination, dates and time of dispatch or receipt of such electronic record are available therein.

This section does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

Moreover, this section does not apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

Section 8 provides for the publication of rules, regulations and notifications in the electronic Gazette. It provides that where any law requires the publication of any rule, regulation, order, bye-law, notification or any other matter in the Official Gazette, then such requirement shall be deemed to be satisfied if the same is published in an electronic form. It also provides where the Official Gazette is published both in the printed as well as in the electronic form, the date of publication shall be the date of publication of the Official Gazette which was first published in any form.

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

Power to Central Government to make rules (Section 10)

This section 10 provides that the Central Government, in respect of Digital Signature may prescribe by rules the following:

a. The type of digital signature
b. The manner and format in which the digital signature shall be affixed.
c. The manner or procedure which facilitates identification of the person affixing the digital signature
d. Control processes and procedures to ensure adequate integrity, security and confidentially of electronic records or payments; and
e. Any other matter which is necessary to give legal effect to digital signatures.

ATTRIBUTION, RECEIPT AND DISPATCH OF ELECTRONIC RECORDS (CHAPTER IV)

The act deals with attribution, receipt and dispatch of electronic records. 'Attribution' with regard to a certain means 'to consider it to be written or made by someone'. Hence, this section lays down how an electronic record is to be attributed to the person who originated it. This is given in section 11.

Section 12 provides for the manner in which acknowledgement of receipt of an electronic record by various modes shall be made.

Section 13 provides for the manner in which the time and place of dispatch and receipt of electronic record sent by the originator shall be identified. It is provided that in general, an electronic record is deemed to be dispatched at the place where the originator has his place of business and received where the addressee has his place of business.

For the purpose of this section,

a. if the originator or the addressee has more than one place of business, the principal place of business shall be the place of business;
b. if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;
c. "usual place of residence", in relation to a body corporate, means the place where it is registered.

SECURE ELECTRONIC RECORDS AND SECURE DIGITAL SIGNATURES (CHAPTER V)

Chapter 5 sets out the conditions that would apply to qualify electronic records and digital signatures as being secure. It contains sections 14 to 16.

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

Section 16 provides for the power of the Central Government to prescribe the security procedure in respect of secure electronic records and secure digital signatures. In doing, so, the Central Government shall take into account various factors like nature of the transaction, level of sophistication of the technological capacity of the parties, availability and cost of alternative procedures, volume of similar transactions entered into by other parties etc.

REGULATION OF CERTIFYING AUTHORITIES (CHAPTER VI)

Chapter 6 contains detailed provisions relating to the appointment and powers of the controller and Certifying authorities. It contains 17 to 34.

Section 17 provides for the appointment of controller and other officers to regulate the certifying Authorities.

Section 18 lays down the functions which the Controller may perform in respect of activities of Certifying Authorities.

Section 19 provides for the power of the Controller with the previous approval of the Central Government to grant recognition to foreign certifying Authorities subject to such condition and restrictions as may be imposed by regulations.

Section 20-this section provides that the Controller shall be acting as repository of all Digital Signature Certificates issued under the Act. He shall also adhere to certain security procedure to ensure secrecy and privacy of the digital signatures and also to satisfy such other standards as may be prescribed by the Central Government. He shall maintain a computerized database of all public keys in such a manner that they are available to the general public.

Section 21-this section provides that a license to be issued to a certifying Authority to issue Digital Signature Certificates by the Controller shall be in such form and shall be accompanied with such fees and other documents as may be prescribed by the Central Government. Further, the Controller after considering the application may either grant the license or reject the application after giving reasonable opportunity of being heard.

Section 22-This section provides that the application for license shall be accompanied by a certification practice statement and statement including the procedure with respect to identification of the applicant. It shall be further accompanied by a fee not exceeding Rs. 25,000 and other documents as may be prescribed by the Central Government.

Section 23 deals with the procedure for grant or rejection of license by the controller on certain grounds.

However, that no application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case.

Section 25 provides that the controller may revoke a license on grounds such as incorrect or false material particulars being mentioned in the application and also on the ground of contravention of any provisions of the Act, rule, regulation or order made thereunder.

However, no license shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation.

Also, no license shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.

Thereafter, the controller shall publish a notice suspension or revocation of license as the case may be in the database maintained by him.

Further, the database containing the notice of such suspension or revocation, as the case may be, shall be made available through a web site which shall be accessible round the clock. It is also provided that the Controller may, if he considers necessary, publicise the contents of Database in such electronic or other media, as he may consider appropriate

Controller's power to delegate

Under section 27 the controller may in writing authorize the Deputy Controller, Assistant Controller or any officer to exercise any of his powers under the Act.

Other powers

The controller shall have power to investigate contravention of the provisions of the Act or the rules or regulations made thereunder either by himself or through any officer authorised in this behalf.

The controller or any person authorized by hi, 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 the rules or regulations is being committed,

Duties of certifying authorities (Section 30):

1. This section provides that every certifying Authority shall follow certain procedures in respect of Digital Signatures as given below:
   a. Make use of hardware, software, and procedures that are secure from intrusion and misuse;
   b. Provide a reasonable level of reliability in services which are reasonably suited to the performance of intended functions
   c. Adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured and
   d. Observe such other standards as may be specified by regulations.

2. Every Certifying Authority shall also ensure that every person employed by him complies with the provisions of the Act, or rules, regulations or orders made three under.
3. A certifying Authority must display its license at a conspicuous place of the premises in which it carries on its business and a Certifying Authority whose license is suspended or revoked shall immediately surrender the license to the Controller.
4. Section 34 further provides that every Certifying Authority shall disclose its Digital Signature Certificate which contains the public key corresponding to the private key used by that Certifying Authority and other relevant facts.

DIGITAL SIGNATURE CERTIFICATION (CHAPTER VII)

Chapter 7 of the Act contain Section 35 to 40.

Section 35 lays down the procedure for issuance of a Digital Signature Certificate. It provides that an application for such certificate shall be made in the prescribed form and shall be accompanied by a fee not exceeding Rs. 25,000. The fee shall be prescribed by the Central Government, and different fees may be prescribed for different classes of applicants.

The section also provides that no Digital Signature Certificate 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 Digital Signature Certificate;
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:

however, no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

While issuing a Digital Signature Certificate the Certifying Authority should certify that it has complied with the provisions of the Act, the rules and regulations made there under and also with other conditions mentioned in the Digital Signature Certificate.

Suspension of digital Certificate

The Certifying Authority may suspend such certificate if it is of the opinion that such a step need to be taken in public interest.

Such certificate shall not be suspended for a period exceeding 15 days unless the subscriber has been given an opportunity of being heard.

Section 38 provides for the revocation of Digital Signature Certificates under certain circumstances. Such revocation shall not be done unless the subscriber has been given an opportunity of being heard in the matter. Upon revocation or suspension, the certifying Authority shall publish the notice of suspension or revocation of a Digital Signature Certificate.

DUTIES OF SUBSCRIBERS (Chapter VIII)

This chapter contains sections 40 to 42. It specifies duties of subscribers.

1. On acceptance of the Digital Signature Certificate the subscriber shall generate a key pair using a secure system.

   A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorises the publication of such signature to one or more persons or otherwise demonstrates his approval of the Digital Signature Certificate. By so accepting the certificate, the subscriber certifies to the public the following.
   a. that he holds the private key corresponding to the public key listed in the Digital signature certificate; and
   b. that all the information contained in the certificate as well as material relevant to them are true.
   c. The subscriber shall exercise all reasonable care to retain control of his private key corresponding to the public key. If such private key has been compromised (i.e., endangered or exposed), the subscriber must immediately communicate the fact to the Certifying Authority.

Otherwise, the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

PENALTIES AND ADJUDICATION (Chapter IX)

Chapter 9 contains sections 43 to 47. It provides for awarding compensation or damages for certain types of computer frauds. It also provides for the appointment of Adjudicating officer for holding an inquiry in relation to certain computer crimes and for awarding compensation.

Types of penalties

Sections 43 to 45 deal with different nature of penalties.

Section 43 deals with penalty for damage to computer, computer system, etc by any of the following methods:

a. securing access to the computer, computer system or computer network;
b. downloading or extracting any data, computer database or information from such computer system or those stored in any removable storage medium
c. introducing any computer contaminant or computer virus into any computer, computer system or network.
d. Damaging any computer, computer system or network or any computer data, database or program
e. Disrupting any computer, computer system or network
f. Denying access to any person authorized to access any computer, computer system or network.
g. Providing assistance to any person to access any computer, computer system or network in contravention of any provisions of this Act or its Rules.
h. Charging the services availed of by one person to the account of another person by tampering with or manipulating any computer, computer system or network.

Explanation-for the purposes of this section,

1. "computer contaminant" means any set of computer instructions that are designed-
   a. to modify, destroy, record, transmit data or program residing within a computer, computer system or computer network; or
   b. by any means to usurp the normal operation of the computer, computer system, or computer network;
2. "computer database" 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 computer network and are intended for use in a computer, computer system or computer network;

3. "computer virus" means any computer instruction, information, data of program that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a program, data or instruction is executed or some other even takes place in that computer resource;
4. "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

Section 46 confers the power to adjudicate contravention under the Act to an officer not below than the rank of a Director to the Government of India or an equivalent officer or a State Government. Such appointment shall be made by the Central Government. In order to be eligible for appointment as an adjudicating officer, a person must possess adequate experience in the filed of Information Technology and such legal or judicial experience as may be prescribed by the Central Government. The adjudicating officer so appointed shall be responsible for holding an inquiry in the prescribed manner after giving reasonable opportunity of being heard and thereafter, imposing penalty where required.

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

CYBER REGULATIONS APPLATE TRIBUNAL (Chapter X)

The "Cyber Regulations Appellate Tribunal" has appellate powers in respect of orders passed by any adjudicating officer. Civil courts have been barred from entertaining any suit or proceedings in respect of any matter which an adjudicating officer or Tribunal is empowered to handle.

Section 48 provides for establishment of one or more Appellate tribunals to be known as Cyber Regulations Appellate Tribunals.

The Cyber Regulations Appellate Tribunal shall consist of one person only (called the Presiding Officer of the Tribunal) who shall be appointed by notification by the central Government. Such a person must be qualified to be judge of High Court or is or has been a member of the Indian Legal Service in the post in Grade 1 of that service for at least three years.

The Presiding Officer shall hold office for a term of five years or upto a maximum age limit of 65 years, whichever is earlier.

Section 52 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 of Cyber Regulations Tribunal. The Central Government shall appoint another person in accordance with the provisions of this Act.

Resignation and removal of the Presiding Officer (Section 54)

The Presiding Officer shall, unless be is permitted by the Central Government to relinquish his office sooner, continue to hold office until the expiry of three months from the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his term of office, whichever is the earliest.

No order appointing any Presiding Officer shall be called in question merely on the ground of any defect in the Constitution of the Tribunal.

The Central Government shall provide such officers for the functioning of the Cyber Regulations Appellate Tribunal. It empowers the Central Government to frame rules relating to salaries, allowances and other conditions of service of such officers and employees.

Appeal to Cyber Regulations Appellate Tribunal :- An appeal may be made by an aggrieved person against an order made by an adjudicating officer to the Cyber Appellate Tribunal. The appeal must be made within forty five days from the date on which the order is received.

The Cyber Appellate Tribunal may entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period. However, no appeal shall be entertained if the original order was passed with the consent of both parties.

The Tribunal, after giving both the parties an opportunity of being heard, shall pass the order as it thinks fit.

Power and procedures of the Appellate Tribunal

Section 58 provides for the procedure and power of the Cyber Appellate Tribunal. The Tribunal shall also have the powers of the Civil Court under the Code of Civil Procedure, 1908.

Some of the powers specified are in respect of the following matters:

a. summoning and enforcing the attendance of any person and examining him on oath.
b. Requiring production of documents and other electronic records
c. Receiving evidence of affidavits
d. Reviewing its decisions
e. Issuing commissions for examination of witness, etc.

The appellant may either appear in person or may be represented by a legal practitioner to present his case before the Tribunal.

Section 60 provides for period of limitation for admission of appeals from the aggrieved persons to the Cyber Appellate Tribunal.

Section 61 provides that no court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer has jurisdiction to determine.

Appeal to High Court(Section 62)

This section provides for an appeal to the High Court by an aggrieved person from the decision of the Cyber Appellate Tribunal. The appeal shall be made within sixty days from the date on which the tribunal's decision is communicated. The appeal shall be on any question of law or fact arising out o f the order.

Compounding of contravention

Section 63-This Section provides that any contravention under the Act may be compounded by the Controller or adjudication officer, either before or after the institution of the adjudication proceedings subject to such conditions as he may impose.

It is also provided that such sum shall not, in any case, exceed the maximum amount of the penalty which may be imposed under this Act for the contravention so compounded. However, these provisions shall not apply to a person who commits the same or similar contravention within a period of three years from the date on which the first contravention, committed by him, was compounded.

Recovery of Penalty

Section 64 provides for recovery of penalty as arrears of land revenue and for suspension of the license or Digital Signature Certificate till the penalty is paid.

OFFENCES (CHAPTER XI)

Chapter 11 deals with some computer crimes and provides for penalties for these offences. It contains sections 65 to 78.

Tampering with computer source documents

This section provides for punishment with imprisonment up to three years or with a fine which may extend to Rs. 2 lakhs or with both whoever knowingly or intentionally tampers with the computer code source documents.

"Computer source code" means the listing of programs, computer commands, design and layout and program analysis of computer resource in any form.

Hacking with computer system:

'Hacking' is a term used to describe 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 the public or that person. Section 66 provides that a person who commits hacking shall be punished with a fine upto Rs. 2 lakhs or with imprisonment upto 3 years, or with both.

Publishing of information which is obscene in electronic form

Section 67 provides for punishment to whoever transmits or publishes or causes to be published or transmitted, any material which is obscene in electronic form with imprisonment for a term which may extend to five years and with fine which may extend to Rs. 1 lakh on first conviction. In the event of second or subsequent conviction the imprisonment would be for a term which may extend to ten years and fine which may extend to Rs. 2 lakhs.

Power of the controller

1. Section 68 provides that the Controller may give directions to a certifying Authority or any employee of such authority to take such measures or cease carrying on such activities as specified in the order, so as to ensure compliance with this law. If any person fails to comply, he shall be liable to imprisonment upto 3 years or five upto Rs. 2 laksh, or both.
2. Section 69 empowers the Controller, if he is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, security of the State, friendly relation with foreign states or public order, to intercept any information transmitted through any computer system or computer network.
3. Section 70 empowers the appropriate Government to declare by notification any computer, computer system or computer network to be a protected system. Any unauthorized access of such systems will be punishable with imprisonment which may extend to ten years or with fine.

Penalty for Misrepresentation

This section provides that any person found misrepresenting or suppressing any material fact from the Controller or the Certifying Authority shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to Rs. 1 lakh or with both.

Penalty for breach of confidentiality

Section 72 provides a punishment for breach of confidentiality and privacy of electronic records, books, information, etc. by a person who has access to them without the consent of the person to whom they belong with imprisonment for a term which may extend to two years or with fine which may extend to Rs. 1 lakh or with both.

Penalty for publishing false Digital Signature Certificate

[Section 73]- this section provides punishment for publishing a Digital Signature Certificate false in material particulars or otherwise making it available to any other person with imprisonment for a term which may extend to two years or with fine which may extend to Rs 1 lakh or with both.

Penalty for fraudulent publication

This section provides for punishment with imprisonment for a term which may extend to two years or with fine which may extend to Rs. 1 lakh or with both to a person whoever knowingly publishes for fraudulent purpose any Digital Signature Certificate.

Act to apply for offence committed outside India

Section 75 provides for punishment for commission of any offence or contravention by a person outside India irrespective of his nationality if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

Confiscation (Section 76)

This section provides for confiscation of any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto in respect of contravention of any provision of the Act, rules, regulations or orders made thereunder.

It is also provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made thereunder, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorised by this Act against the person contravening the provisions of this Act, rules, orders or regulations made thereunder as it may think fit.

Section 77 further provides that penalty and confiscation provided under this Act shall not interfere with other punishments provided under any other law for the time being in force.
Section 78 provides for power to investigate the offences under the Act by a police officer not below the rank of Deputy Superintendent of police.

NETWORK SERVICE PROVIDERS NOT TO BE LIABLE IN CERTAIN CASES (CHAPTER XII)

CHAPTER XII contains section 79 which provides that the Network Service Providers shall be liable for any third party information or data made available by him if he proves that the offence, was committed without his knowledge or consent.

Explanation-for the purposes of this section,--

a. "network service provider" means an intermediary;
b. "third party information" means any information dealt with by a network service provider in his capacity as an intermediary;

MISCELLANEOUS (CHAPTER XIII)

Power of Central Government to make rules

Section 87 of the Act confers on the Central Government the power to make rules by notifying in the Official Gazette and the Electronic Gazette, in respect of certain matters, some of which are:

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

Every notification made by the Central Government shall be laid, as soon as possible after it is made, before each House of Parliament, while it is in session, for a total period of thirty days. This period may be comprised in one session or in two or more successive sessions. If before the expiry of the session immediately following the above period, both House agree in making any modification, the rule will thereafter have effect only in the modified form. Similarly, if both Houses agree that the rule should not be made, the notification shall have no effect, thereafter.

Power of State Government to make rules

The State Government may by notification in the Official Gazette, make rules to carry out the provisions of this Act. Such rules may provide for all or any of 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 signatures in Government and its agencies.
2. The manner and format in which such electronic records shall be filed or issued and the fee or charges in connection of the same.
3. Any other matter required to be provided by rules by the State Government. Every such rule shall be laid before each House of the State Legislature.

Cyber Regulations Advisory Committee

The Cyber Regulations Advisory Committee shall be constituted by the Central Government. It shall consist of a chairperson and such member of official and non-official members as the Central Government shall deem fit. Such members shall have special knowledge of the subject matter of the interests principally affected. The Committee shall advise the Central Government on the rules or any other purpose connected with the Act and the Controller in framing regulations under this Act.

Power of Controller to make regulations

The controller has been given powers under Section 89 to make regulations consistent with the Act and the related rules so as to carry out the purposes of this Act. However, he may do so after consultation with the Cyber Regulations Advisory Committee and with the previous approval of the Central Government. These regulations shall be notified in the Official Gazette. These regulations shall be related to the following matters:

1. the particulars relating to maintenance of data base containing the disclosure record of every Certifying Authority
2. the conditions and restrictions subject to which the Controller may recognise 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 under Section 34.
6. The particulars of statement to be submitted along with an application for the issue of a Digital Signature Certificate
7. The manner in which the subscriber should communicate the compromise of private key to the Certifying Authority.

The procedure for passing the resolution is the same as given in section 87 in respect of notifying rules by the Central Government.

Power of police officer and other officers to enter, search etc.

Section 80 provides, that not withstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a Deputy Superintendent of Police, or any other officer of the Central or State Government, if so authorised by the Central Government, may enter any public place 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.

For this purpose, 'public place' would include a public conveyance, any hotel, any shot or any other place accessible to the public.

The section further provides that where any person is arrested by an officer other than a police officer, such officer shall immediately send the arrested person to a magistrate having jurisdiction or to the officer in charge of a police station.

Liability of companies (Section 85)

Where a company commits any offence under this Act or any rule thereunder, every person who, at the time of the contravention, was in charge of and was responsible for the conduct of the business, of the company shall be guilty of the contravention. However, he 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.

Further where a contravention has been committed by a company, and it is proved that the contravention took place with the connivance or consent of or due to any 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 be proceeded against and punished accordingly.

For the purposes of this section, 'company' includes a firm or other association of persons and 'director' in relation to a firm means a partner in the firm.

The Information Technology Act will go a long way in facilitating and regulating electronic commerce. It has provided a legal framework for smooth conduct of e-commerce. It has tackled the following legal issues associated with e-commerce.

a. requirement of a writing;
b. requirement of document;
c. requirement of a signature; and
d. requirement of legal recognition for electronic messages, records and documents to be admitted in evidence in a court of law.

However, the Act, has not addressed the following areas:

1. protection for domain names
2. infringement of copyright laws
3. jurisdiction aspect of electronic contracts
4. taxation of goods and services traded through e-commerce and
5. stamp duty aspect of electronic contracts.

CHAPTER 17

AUDIT OF INFORMATION SYSTEMS

INTRODUCTION

Organizations continue to rely more and more on computer technology. Although the initial use of computers only involved a conversion from manual to automatic transaction processing to increase productivity and decrease cost, the current use of computers is changing the way business operates. The computer is such an integral part of day-to-day operations in most organizations, that when the computer is not functioning the business cannot perform its routine transactions.

The rate of change in computer technology is accelerating. As computerized applications are growing in size, there is a major trend to build and move applications to client/server technology. Organizations are mixing hardware platforms from different vendors with a combination of commercially available software and in-house developed software. As a result of these changes, business risk increases. EDP auditing is needed to evaluate the adequacy of automated information systems to meet processing needs, to evaluate the adequacy of internal controls, and to ensure that assets controlled by those systems are adequately safeguarded. This chapter gives a general overview of the process of information system audit.

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-not just the computerized segment. This requires their involvement from the time that a transaction is initiated until it is posted to the organization's general ledger. Specifically, auditors must ensure that provisions are made for:

- an adequate audit trail so that transactions can be traced forward and backward through the system.
- Controls over the accounting for all data (i.e. transactions) entered into the system and controls to ensure the integrity of those transactions throughout the computerized segment of the system.
- Handling exceptions to and rejections from the computer system.
- Testing to determine whether the systems perform as stated.
- Control over changes to the computer system to determine whether the proper authorization has been given.
- Authorization procedures for system overrides.
- Determining whether organization and government policies and procedures are adhered to in system implementation.
- Training user personnel in the operation of the system.
- Developing detailed evaluation criteria so that it is possible to determine whether the implemented system has met predetermined specifications.
- Adequate controls between interconnected computer systems.
- Adequate security procedures to protect the user's data.
- Backup and recovery procedures for the operation of the system.
- Technology provided by different vendors (i.e. operational platforms) are compatible and controlled.
- Data bases are adequately designed and controlled to ensure that common definitions of data are used throughout the organization, that redundancy is eliminated or controlled, and that data existing in multiple data bases is updated concurrently.

This list affirms that the auditor is primarily concerned with adequate controls to safeguard the organization's assets.

The Computer Auditing Approach: The audit methods that are effective for manual audits prove ineffective in many IS audits because of these factors:

- *Electronic evidence*--Essential evidence is not physically retrievable by most auditors, and it is not readable in its original electronic form.

- *Terminology*—The tools and techniques used in automated applications are described in terms that are difficult for the non-EDP auditor to understand.
- *Automated processes*—The methods of processing are automated rather than manual, making it difficult for the non-EDP auditor to comprehend processing concepts and the logic of these concepts.
- *New risks and controls*—Threats to computer systems and the countermeasures to those threats (i.e. controls) are new to non-EDP auditors, and the magnitude of the risks and the effectiveness of the controls are not understood.
- *Reliance of controls*—In manual systems, the auditor can place some reliance on hard-copy evidence, regardless of the adequacy of the controls. Whereas, in automated systems, the electronic evidence is only as valid as the adequacy of controls.

Because the rate of these changes varies among systems in organizations, the methods and approaches of auditing automated information systems differ among applications and organizations. For example, some organizations still rely heavily on hard-copy evidence, and others have eliminated much of it.

The IS Audit's scope and objectives: To evaluate whether an IS audit is successful, first, the auditor must clearly identify the intended scope and objectives of the audit. The IS auditor may focus on one or more of the review areas discussed in the following sections.

Computerized Systems and Applications: The auditor should verify that systems and applications are appropriate to the user needs, efficient, and adequately controlled to ensure valid, reliable, timely, and secure input, processing, and output at current and projected levels of systems activity.

Information Processing Facilities: The information processing facility must be controlled to ensure timely, accurate, and efficient processing of applications under normal and potentially disruptive conditions.

Systems Development: An IS auditor should ensure that systems under development meet the objectives of the organization, satisfy user requirements, and provide efficient, accurate, and cost-effective systems and applications. The auditor should also ensure that these systems are written, tested, and installed in accordance with generally accepted standards for systems development.

Management of Information Systems: Information systems management must develop an organizational structure and procedures to ensure a controlled and efficient environment for information processing. This plan should also specify the computers and peripheral equipment required to support all functions in an economic and timely manner.

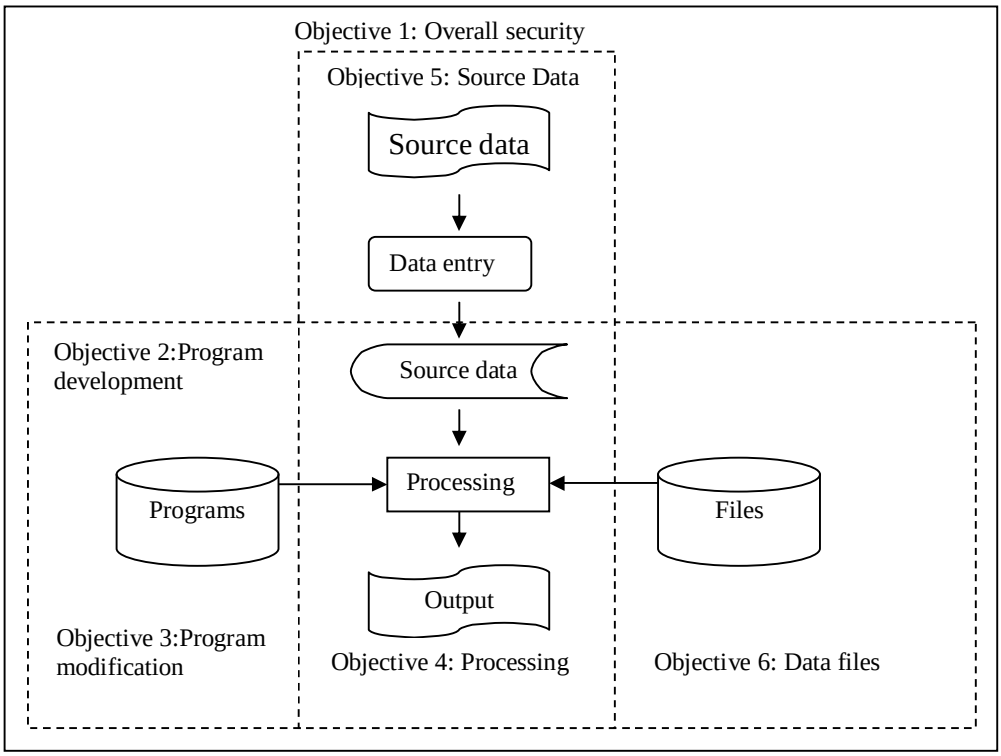
Client/Server, Telecommunications, and Intranets: Many companies are decentralizing their traditional mainframe information processing facilities into local area networks (LANs), wide area networks (WANs), value added networks (VANs), client/server, and Internet/Internet systems. In a client/server environment, all applications that can be dedicated to a user are put on the client. All resources that need to be shared are put on the server. Auditors must ensure that controls are in place on the client (i.e., the computer receiving services) as well as on the server (i.e., the computer providing services) and on the network (i.e., the supporting WANs and VANs) connecting clients and servers. In an internet/Internet environment, the network provides both application and data to clients from the Intranet server. Auditors must provide the same level of control assurance in an Internet/Intranet environment as in a client/server environment, with special emphasis on two key Internet/Intranet protocols: transmission control protocol/Internet protocol (TCP/IP) and hypertext transfer protocol (HTTP)

The IS Auditor's Role:

The purpose of an AIS audit is to review and evaluate the internal controls that protect the system. When performing an IS audit, auditors should ascertain that the following objectives are met:

1. Security provisions to protect computer equipment, programs, communications, and data from unauthorized access, modification, or destruction.
2. Program development and acquisition is performed in accordance with management's general and specific authorization.
3. Program modifications have the authorization and approval of management.
4. Processing of transactions, files, reports, and other computer records is accurate and complete.
5. Source data that is inaccurate or improperly authorized is identified and handled according to prescribed managerial policies.
6. Computer data files are accurate, complete, and confidential.

Following diagram depicts the relationship among these six objectives and IS components. Each of these objectives is now discussed in detail. Each description includes an audit plan to accomplish each objective, as well as the techniques and procedures necessary for carrying out the plan.



Information systems components and related IS Audit objectives

COMPUTER SECURITY

Given below table contains a framework for auditing computer security. It shows the following:

1. *Types of security errors and fraud faced by companies:* These include accidental or intentional damage to system assets: unauthorized access, disclosure, or modification of data and programs: theft; and interruption of crucial business activities.

2. *Control procedures to minimize security errors and fraud:* These include developing an information security/protection plan, restricting physical and logical access, encrypting data, protecting against viruses, implementing firewalls, instituting data transmission controls, and preventing and recovering from system failures or disasters.

3. *Systems review audit procedures:* These include inspecting computer sites; interviewing personnel; reviewing policies and procedures: and examining access logs, insurance policies, and the disaster recovery plan.
4. *Tests of controls audit procedures:* Auditors test security controls by observing procedures verifying that controls are in place and work as intended, investigating errors or problems to ensure they were handled correctly, and examining any tests previously performed. For example, one way to test logical access controls is to try to break into a system. During one of the government agency security audit, auditors used agency terminals to gain unauthorized access to its computer system, disabled its security-checking procedures, and controlled the system from the terminal. The security breakdown was possible because of poor administrative controls and inadequate security software.
5. *Compensating controls:* If security controls are seriously deficient, the organization faces substantial risks. Sound personnel policies and effective segregation of incompatible duties can partially compensate for poor computer security. Good user controls will also help, if user personnel can recognize unusual system output. However, it is unlikely that these controls can compensate indefinitely for poor computer security. Hence, auditors should strongly recommend that security weaknesses be corrected.

TABLE: Framework For Audit Of Computer Security

Types of Errors and Fraud

- Theft of or accidental or intentional damage to hardware and files
- Loss or theft of or unauthorized access to programs, data files and other system resources.
- Loss or theft of or unauthorized disclosure of confidential data.
- Unauthorized modification or use of programs and data files.
- Interruption of crucial business activities.

Control Procedures

- Information security/protection plan.
- Restrictions on physical access to computer equipment.
- Logical access controls based on password protection and other authentication procedures.
- Data storage and transmission controls such as encryption.
- Virus protection procedures.
- File backup and recovery procedures.
- Fault-tolerant systems design.
- Disaster recovery plan.
- Preventive maintenance.
- Firewalls.
- Information systems insurance.

Audit Procedures: System Review

- Inspect computer sites.
- Interview IS personnel about security procedures
- Review written documentation about physical access policies and procedures
- Review logical access policies and procedures.
- Review file backup and recovery policies and procedures
- Examine data storage and transmission policies and procedures.
- Review procedures employed to minimize system downtime.
- Examine system access logs.
- Examine disaster recovery plan.
- Examine casually insurance policies.

Audit Procedures: Tests of Controls

- Observe computer site access procedures.
- Observe the preparation and 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 use.
- Verify the effective use of data transmission controls.
- Verify the effective use of firewalls.
- Verify the use of preventive maintenance and un interruptible power.
- Verify amounts and limitations on insurance coverage.
- Examine the results of tests simulations of disaster recovery plan.

Compensating Controls

- Sound personnel policies.
- Effective user controls.
- Segregation of incompatible duties.

PROGRAM DEVELOPMENT AND ACQUISITION

Following table provides a framework for reviewing and evaluating the program development process. Two things can go wrong in program development:

1. inadvertent errors due to misunderstanding system specifications or careless programming, and
2. unauthorized instructions deliberately inserted into the programs. These problems can be controlled by requiring both management and user authorization and approval, thorough testing, and proper documentation.

TABLE: Framework for Audit Program Development

Types of Errors and Fraud

- Inadvertent programming errors.
- Unauthorized program code.

Control Procedures

- Management authorization for program development and approval of programming specifications.
- User approval of programming specifications.
- Through testing of new programs.
- User acceptance testing.
- Complete systems documentation, including approvals.

Audit Procedures: System Review

- Independent and concurrent review of the systems development process.
- Review systems development policies and procedures.
- Review systems authorization and approval procedures.
- Review programming evaluation standards.
- Review program documentation standards.
- Review program testing and test approval procedures.
- Discuss systems development procedures with management, system users, and IS personnel.
- Review final application system documentation.

Audit Procedures: Tests of Controls

- Interview users about their involvement in systems design and implementation.
- Review minutes of development team meetings for evidence of involvement.
- Verify management and user sign-off at milestone points in the development process.
- Review test specifications, test data, and results of systems tests.

Compensating Controls

- Strong processing controls.
- Independent processing of test data by auditor.

The auditor's role in systems development should be limited to an independent review of systems development activities. To maintain the objectivity necessary for performing an independent evaluation function, auditors should not be involved in developing the system. During the systems review, auditors should gain an understanding of development procedures by discussing them with management, system users, and IS personnel.

To test systems development controls, auditors should interview managers and system users, examine development approvals, and review the minutes of development team meetings. The auditor should review thoroughly all documentation relating to the testing process and ascertain that all program changes were tested. The auditor should examine the test specifications, review the test data, and evaluate the test results. If unexpected test results were obtained, the auditor should ascertain how the problem was resolved.

Strong processing controls (see objective 4) sometimes can compensate for inadequate development controls. If compensatory processing controls are relied on, the auditor should obtain persuasive evidence of compliance, using techniques such as independent processing of test data. If this type of evidence cannot be obtained, the auditor may have to conclude that a material weakness in internal control exists and that the risk of significant errors or fraud in application programs is unacceptably high.

PROGRAM MODIFICATION

Table below presents a framework for auditing application programs and system software changes. The same errors and frauds that can take place during program changes can happen during program development. For example, one programmer assigned to modify his company's payroll system inserted a command to erase all company files if a termination notice was ever entered into his own payroll record. When the programmer was fired, his termination notice caused the system to crash and erased key files.

When a program change is submitted for approval, a list of all required updates should be compiled and then approved by management and program users. All program changes should be thoroughly tested and documented. During the change process, the development version of the program must be kept separate from the production version. After the method program has received final approval, the change is implemented by replacing the production version with the developmental version.

During system review, auditors should gain an understanding of the change process by discussing it with management and user personnel. The policies, procedures, and standards for approving, modifying, testing, and documenting the changes should be examined. A complete set of final documentation materials for recent program changes. Including test procedures and results, should be reviewed. Finally the auditor should review the procedures used to restrict logical access to the developmental version of the program.

TABLE: Framework for Audit of Program Modification Procedures

Types of Errors and Fraud

- Inadvertent programming errors.
- Unauthorized program code.

Control Procedures

- Listing of program components that is to be modified.
- Management authorization and approval of program modifications.
- User approval of program change specifications.

- Thorough testing of program changes, including user acceptance test.
- Complete program change documentation, including approvals.
- Separate development, test, and production versions of program.
- Changes implemented by personnel independent of users and programmers.
- Logical access controls.

Audit Procedures: System Review

- Review program modification policies, standards and procedures.
- Review documentation standards for program modification.
- Review program modification testing and test approval procedures.
- Discuss program modification policies and procedures with management, system users, and IS personnel.
- Review final documentation for some typical program modifications.
- Review test specifications, test data, and results of systems tests.
- Review logical access control policies and procedures.

Audit procedures: Tests of Controls

- verify user and IS management approval for program changes.
- Verify that program components to be modified and identified and listed.
- Verify that program change tests procedures comply with standards.
- Verify that program change documentation complies with standards.
- Verify that logical access controls are in effect for program changes.
- Observe program change implementation and verify that
  -Separate development, test, and production versions are maintained.
  -Changes are not implemented by either user or programming personnel.
- to test for unauthorized or erroneous program changes, use
  -Source code comparison program
  -Reprocessing
  -Parallel simulation

Compensating Controls

- Independent audit tests for authorized or erroneous program changes.
- Strong processing controls.

An important part of an auditor's tests of controls is to verify that program changes were identified, listed, approved, tested, and documented. This step requires that the auditor observe how changes are implemented in order to verify that separate development and production programs are maintained and that changes are implemented by someone independent of the user and programming functions. The auditor should review the development program's access control table to verify that only those users assigned to carry out the modification has access to the system.

To test for unauthorized program changes, auditors can use a source code comparison program. After auditors thoroughly test a newly developed program they keep a copy of its source code. At any subsequent time, the auditor may use the comparison program to compare the current version of the program with the original source code. If no changes have been authorized these two versions should be identical, source code. If no changes have been authorized, these two versions should be identical. Therefore any unauthorized differences should result in an investigation. If the difference represents an authorized change, the auditor can refer to the program change specifications to ensure that the changes were authorized and correctly incorporated.

Two additional techniques detect unauthorized program changes. The reprocessing technique also uses a verified copy of the source code. On a surprise basis, the auditor uses the program to reprocess data and compare that output with the company's data. Discrepancies in the two sets of output are

investigated to ascertain their cause. Parallel simulation is similar to reprocessing except that the auditor writes a program instead of saving a verified copy of the source code. The auditor's results are compared with the company's and any differences are investigated. Parallel simulation can be used to test a program during the implementation process.

Auditors should observe the testing and implementation, review related authorizations and documents, and, if necessary, perform independent tests for each major program change. If this step is skipped and program change controls are subsequently determined to be inadequate, it may not be possible to rely on program outputs. In addition, auditors should always test programs on a surprise basis as a precaution against unauthorized program changes being inserted after the examination is completed and then removed just prior to the next scheduled audit.

If internal controls over program changes are deficient, a compensating control is source code comparison, reprocessing, or parallel simulation performed by the auditor. In addition, the presence of sound processing controls, independently tested by the auditor, can partially compensate for such deficiencies. However, if the deficiencies are caused by inadequate restrictions on program file access, the auditor should strongly recommend actions that will strengthen the organization's logical access controls.

COMPUTER PROCESSING

Table below provides a framework for auditing computer processing controls. The focus of the fourth objective is the processing of transactions, files, and related computer records to update files and databases and to generate reports.

During computer processing the system might fail to detect erroneous input, improperly correct input errors, process erroneous input, or improperly distribute or disclose output. The control procedures to detect and prevent these errors and the systems review and tests of controls procedures which the auditor employs are shown in the Table. 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.

Auditors must periodically re-evaluate processing controls to ensure their continued reliability. If processing controls are unsatisfactory, user and source data controls may be strong enough to compensate. If not, a material weakness exists and steps should be taken to eliminate the control deficiencies.

Several specialized techniques allow the auditor to use the computer to test processing controls. They include processing test data, using concurrent audit techniques, and analyzing program logic. Each of these procedures is explained next.

Test Data Processing: One way to test a program is to process a hypothetical series of valid and invalid transactions. The program should process all of the valid transactions correctly and identify and reject all of the invalid ones. All logic paths should be checked for proper functioning by one or more of the test transactions. Examples of invalid data include records with missing data, fields containing unreasonably large amounts, invalid account numbers or processing codes, non-numeric data in numeric fields, and records out of sequence.

Several resources are available when preparing test data. For example:

- A listing of actual transactions.
- The test transactions that the programmer used to test the program.
- **A test data generator program,** which automatically prepares test data based on program specifications.

Although processing of test transactions is usually effective, it does have the following disadvantages:

1. The auditor must spend considerable time developing an understanding of the system and preparing an adequate set of test transactions.
2. Care must be taken to ensure that test data does not affect the company's files and data bases. The auditor can reverse the effects of the test transactions or process the transactions in a separate run using a copy of the file or data base. However, a separate run removes some of the authenticity obtained from processing test data with regular transactions. Also, since the reversal procedures may reveal the existence and nature of the auditor's test to key personnel, it can be less effective than a concealed test.

Concurrent Audit Techniques: Millions of rupees of transactions can be processed in an on-line system without leaving a satisfactory audit trail. In such cases, evidence gathered after data processing is insufficient for audit purposes. In addition, since many on-line systems process transactions continuously, it is difficult or impossible to stop the system in order to perform audit tests. Thus, the auditor uses concurrent audit techniques to continually monitor the system and collect audit evidence while live data are processed during regular operating hours. Concurrent audit techniques use embedded audit modules, which are segments of program code that performs audit functions. They also report test results to the auditor and store the evidence collected for the auditor's review.

Auditors commonly use five concurrent audit techniques.

i) An integrated test facility (ITF) technique places a small set of fictitious records in the master files. The records might represent a fictitious division, department, or branch office or a customer or supplier. Processing test transactions to update these dummy records will not affect the actual records. Because fictitious and actual records are processed together, company employees usually remain unaware that this testing is taking place. The system must distinguish ITF records from actual records, collect information on the effects of the test transactions, and report the results. The auditor compares processing and expected results in order to verify that the system and its controls are operating correctly.

ITF is well suited to testing on-line processing systems because test transactions can be submitted on a frequent basis, processed with actual transactions, and traced throughout every processing stage. All this can be accomplished without disrupting regular processing operations. However, care must be taken not to combine dummy and actual records during the reporting process.

ii) *The snapshot technique* examines the way transactions are processed. Selected transactions are marked with a special code that triggers the snapshot process. Audit modules in the program record these transactions and their master file records before and after processing. Snapshot data are recorded in a special file and reviewed by the auditor to verify that all processing steps have been properly executed.

iii) *SCARF (system control audit review file)* uses embedded audit modules to continuously monitor transaction activity and collect data on transactions with special audit significance. The data are recorded in a SCARF file or **audit log.** Transactions that might be recorded in a SCARF file include those exceeding a specified rupee limit, involving inactive accounts, deviating from company policy, or containing write-downs of asset values. Periodically the auditor receives a printout of the SCARF file, examine the information to identify any questionable transactions, and performs any necessary follow-up investigation.

iv) *Audit hooks* are audit routines that flag suspicious transactions. For example, internal auditors at an Insurance Company determined that their policy holder information system was vulnerable to fraud every time a policyholder changed his or her name or address and then subsequently withdrew funds from the policy. They devised a system of audit hooks to tag records with a name or address change. The internal audit department is now notified when a tagged record is

associated with a withdrawal and can appropriately investigate the transaction for fraud. When audit hooks are employed, auditors can be informed of questionable transactions as soon as they occur. This approach, known as real-time notification, display a message on the auditor's terminal.

v) *Continuous and intermittent simulation (CIS)* embeds an audit module in a data base management system. The CIS module examines all transactions that update the DBMS using criteria similar to those of SCARF. If a transaction has special audit significance, the module independently processes the data (in a manner similar to parallel simulation), records the results, and compares them with those obtained by the DBMS. If any discrepancies exist, the details are written onto an audit log for subsequent investigation. If serious discrepancies are discovered, the CIS may prevent the DBMS from executing the update process.

Analysis of program Logic: If an auditor suspects that a particular application program contains unauthorized code or serious errors, a detailed analysis of the program logic may be necessary. Since this process is time-consuming and requires programming language proficiency, it should be used only as a last resort. To perform the analysis, auditors refer to systems and program flowcharts, program documentation, and a listing of the program source code. The following software packages serve as aids in this analysis:

- Automated flowcharting programs, which interpret program source code and generate a corresponding program flowchart.
- Automated decision table programs, which generate a decision table representing the program logic.
- Scanning routines, which search a program for occurrences of a specified variable name or other character combinations.
- Mapping programs, which identify unexecuted program code. This software could have uncovered the program code the unscrupulous programmer inserted to erase all computer files when he has terminated.
- Program tracing, which sequentially prints all application program steps (line numbers or paragraph names) executed during a program run. This list is intermingled with regular output so auditors can observe the precise sequence of events that unfold during program execution. Program tracing helps auditors detect unauthorized program instructions, incorrect logic paths, and unexecuted program code.

TABLE: Framework For Audit Of Computer Processing Controls.

Types of Errors and Fraud

- Failure to detect incorrect, incomplete, or unauthorized input data.
- Failure to properly correct errors flagged by data editing procedures.
- Introduction of errors into files or data bases during updating.
- Improper distribution or disclosure of computer output
- Intentional or unintentional report inaccuracies.

Control procedures

- computer data editing routines.
- Proper use of internal and external file labels.
- Reconciliation of batch totals.
- Effective error correction procedures
- Understandable operating documentation and run manuals.
- Component supervision of computer operations.
- Effective handling of data input and output by data control personnel.
- File change listings and summaries prepared for user department review.
- Maintenance of proper environmental conditions in computer facility.

Audit Procedures: System Review

- Review administrative documentation for processing control standards.
- Review systems documentation for data editing and other processing controls.
- Review operating documentation for completeness and clarity.
- Review 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.

Audit Procedures: Tests of controls

- Evaluate adequacy of processing control standards and procedures.
- Evaluate adequacy and completeness of data editing controls.
- Verify adherence to processing control procedures by observing computer operations and the data control function.
- Verify that selected application system output is properly distributed.
- Reconcile a sample of batch totals, and follow up on discrepancies.
- Trace disposition of a sample of errors flagged by data edit routines to ensure proper handling.
- Verify processing accuracy for a sample of sensitive transactions.
- Verify processing accuracy for selected computer-generated transactions.
- Search for erroneous or unauthorized code via analysis of program logic.
- Check accuracy and completeness of processing controls using test data.
- Monitor on-line processing systems using concurrent audit techniques.
- Re-create selected reports to test for accuracy and completeness.

Compensating Controls

- Strong user controls.
- Effective source data controls.

SOURCE DATA CONTROLS

Table below shows the internal controls that prevent, detect, and correct inaccurate or unauthorized source data. It also shows the system review and tests of control procedures that auditors use for evaluation. In an on-line system, the source data entry and processing functions are one operation. Therefore, source data controls such as proper authorization and editing data input are integrated with processing controls.

Auditors use an **input controls matrix,** to document the review of source data controls. The matrix shows the control procedures applied to each field on an input record.

Auditors should make sure that the data control function is independent of other functions, maintains a data control log, handles errors, and ensures the overall efficiency of operations. It is usually not economically feasible for small business and PC installations to have an independent data control function. To compensate, user department controls over data preparation, batch control totals, edit programs, restrictions on physical and logical access to the system, and error handling procedures must be stronger. These procedures should be the focus of the auditor's systems review and tests of controls whenever the presence of an independent data control function is absent.

Although source data controls may not change often, the strictness with which they are applied may. Therefore auditors should test them on a regular basis. The auditor tests the system by evaluating samples of source data for proper authorization. A sample of batch controls should be reconciled. A sample of data edit errors should be evaluated to check that they were resolved and resubmitted into the system.

If source data controls are inadequate, user department and computer processing controls may compensate. If not, the auditor should strongly recommend steps to correct the source data control deficiencies.

TABLE: **Framework for Audit of Source Data Controls**

Types of Errors and Fraud

- Inaccurate source data
- Unauthorized source data

Control Procedures

- Effective handling of source data input by data control personnel
- User authorization of source data input
- Preparation and reconciliation of batch control totals.
- Logging of the receipt, movement, and disposition of source data input
- Check digit verification
- Key verification
- Use of turnaround documents
- Computer data editing routines
- File change listings and summaries prepared for user department review
- Effective procedures for correcting and resubmitting erroneous data

Audit Procedures: System Review

- Review documentation about responsibilities of data control function
- Review administrative documentation for source data control standards
- Review methods of authorization and examine authorization signatures
- Review accounting systems documentation to identify source data content and processing steps and specific 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 system users.

Audit Procedures: Tests of Controls

- Observe and evaluate data control department operations and specific data control procedures
- Verify proper maintenance and use of data control log
- Evaluate how items recorded in the error log are dealt with
- Examine samples of accounting source data for proper authorization
- Reconcile a sample of batch totals, and follow up on discrepancies
- Trace disposition of a sample of errors flagged by data edit routines

Compensating Controls

- Strong user controls
- Strong processing controls

DATA FILES

The sixth objective is concerned with the accuracy, integrity, and security of data stored in machine-readable files. Data storage risks include the unauthorized modification, destruction, or disclosure of data. Many of the controls are seriously deficient, especially with respect to physical or logical access or to backup and recovery procedures, the auditor should strongly recommend they be rectified. Given below table summarizes the errors, controls, and audit procedures for this objective.

TABLE: Framework for Audit of Data File Controls

Type of Errors and Fraud

- Destruction of stored data due to inadvertent errors, hardware or software malfunctions, and intentional acts of sabotage or vandalism.
- Unauthorized modification or disclosure of stored data.

Control Procedures

- Secure file library and restrictions on physical access to data files
- Logical access controls using passwords and access control matrix

- Proper use of file labels and write-protection mechanisms
- Concurrent update controls
- Use of data encryption for highly confidential data
- Use of virus protection software
- Maintenance of backup copies of all data files in all off-site location
- Use of checkpoint and rollback to facilitate system recovery

Audit Procedures: System Review

- Review documentation for functions of file library operation
- Review logical access policies and procedures
- Review operating documentation to determine prescribed standards for
  -use of file labels and write-protection mechanisms
  -use of virus protection software
  -System recovery, including checkpoint and rollback procedures
- review systems documentation to examine prescribed procedures for
  -use of concurrent update controls and data encryption
  -control of file conversions
  -Reconciling master files totals with independent control totals
- Examine disaster recovery plan
- Discuss data file control procedures with IS managers and operators

Audit Procedures: Test of Controls

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

Compensating controls

- strong user controls
- effective computer security controls
- strong processing controls

The auditing-by-objectives approach is a comprehensive, systematic, and effective means of evaluating internal controls in an AIS. It can be implemented using an audit procedures checklist for each objective. The checklist should help the auditor reach a separate conclusion for each objective and suggest compensating controls when an objective is not fully achieved. A separate version of the checklist should be completed for each significant application.

Auditors should review system designs while there is still time to adopt their suggestions for control and audit features. Techniques like ITF, snapshot, SCARF, audit hooks, and real-time notification should be incorporated into a system during the design process, rather than as an afterthought. Similarly, most application control techniques are easier to design into the system than to add after the system is developed.

CHAPTER 18
INFORMATION SECURITY

INTRODUCTION

In the computerized information systems, most of the business processes are automated. Organizations are increasingly relying on Information Technology for information and transaction processing. The growth of E-commerce supported by the growth of the Internet has completely revolutionized and reengineered business processes. The information technology innovations such as hardware, software, networking technology, communication technology and ever-increasing bandwidth lead to completely new business models.

All these new business models and new methods assume that the information required by the business managers is available all the time, it is accurate, it is reliable and no unauthorized disclosure of the same is made. Further, it is also assumed that the virtual business organization is up and running all the time on 24*7 basis (24 hours. 7 days a week). However, in reality, the technology-enabled and technology-dependent organizations are more vulnerable to security threats than ever before.

WHY IS INFORMATION SECURITY IMPORTANT?

Organizations depend on timely, accurate, complete, valid, consistent, relevant, and reliable information. Accordingly, executive management has a responsibility to ensure that the organization provides all users with a secure information systems environment.

It is clear that there are not only many direct and indirect benefits from the use of information systems, there are also many direct and indirect risks relating to the information systems. These risks have led to a gap between the need to protect systems and the degree of protection applied. This gap is caused by.

- Widespread use of technology
- Interconnectivity of systems
- Elimination of distance, time, and space as constraints
- Unevenness of technological changes
- Decentralization of management and control
- Attractiveness of conducting unconventional electronic attacks over more conventional physical attacks against organizations; and
- External factors such as legislative, legal, and regulatory requirements for technological developments

Security failures may result in both financial losses and/or intangible losses such as unauthorized disclosure of competitive or sensitive information.

Threats to information systems may arise from intentional or unintentional acts and may come from internal or external sources. The threats may emanate from, among others, technical conditions (program bugs, disk crashes), natural disasters (fires, floods), environmental conditions (electrical surges), human factors (lack of training, errors, and omissions), unauthorized access (hacking), or viruses. In addition to these, other threats, such as business dependencies (reliance on third party communications carriers, outsourced operations, etc.) that can potentially result in a loss of management control and oversight are increasing in significance.

Adequate measures for information security help to ensure the smooth functioning of information systems and protect the organization from loss of embarrassment caused by security failures.

WHAT IS INFORMATION SECURITY?

Security relates to the protection of valuable assets against loss, disclosure, or damage. This concept of security applies to all information. In this context, the valuable assets are the data or information recorded, processed, stored, shared, transmitted, or retrieved from an electronic medium. The data or information is protected against harm from threats that will lead to its loss, inaccessibility, alteration, or wrongful disclosure. The protection is achieved through a layered series of technological and non-technological safeguards such as physical security measures, user identifiers, passwords, smart cards, biometrics, firewalls, etc.

Security Objective: The objective of information security is "the protection of the interests of those relying on information, and the information systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality, and integrity".
For any organizations, the security objective is met when:

- information systems are available and usable when required (availability):
- data and information are disclosed only on those who have a right to know it (confidentiality); and
- data and information are protected against unauthorized modification (integrity).

The relative priority and significance of availability, confidentiality, and integrity vary according to the data within the information system and the business context in which it is used.

What information is sensitive?

The following examples highlight a few of the many factors necessary for a company to succeed. The common threat in each case is the critical information that each generates.

- **Strategic Plans:** Most organizations readily acknowledge that strategic plans are crucial to the success of a company. But do most companies really make an effort to protect these plans?

  Take this example: a competitor learns that a company is testing a new product line in a specific geographic location. The competitor removes its product from that location, creating an illusionary demand for the product. When the positive results of the marketing test are provided to the company's executives, they decide to roll the product out nationwide. Only then did the company discover that in all other geographic regions the competition for their product was intense. The result: the company lost several million dollars as its product sales failed.

- **Business Operations:** Business operations consist of an organization's process and procedures, most of which are deemed to be proprietary. As such, they may provide a market advantage to the organization. This is the case when one company can provide a service profitably at a lower price than the competition. A company's client lists and the prices charged for various products and services can also be damaging in the hands of a competitor.

  While most organizations prohibit the sharing of such data, carelessness often results in its compromise. Such activity includes inadvertent storage of data on unauthorized systems, unprotected laptops, and failure to secure magnetic media.

- **Finances:** Financial information, such as salaries and wages, are very sensitive and should not be made public. While general salary ranges are known within industry sectors, precise salary information can provide a competitive edge. As salaries and wage-related changes normally comprise the majority of fixed costs, lower costs in this area contribute directly to an organization's profitability. When a competitor knows specific information about a company's wages, the competitor may be able to price its products accordingly. When competitor's costs are lower, they can either under-price the market or increase profits. In either case, the damage to an organization may be significant.

Establishing better information protection: The examples above highlight only three of the various types of sensitive information every business holds. Protecting this information is crucial to the overall success or failure of a company. Businesses hold such a vast array of data, what steps do they need to keep all of their critical information protected?

These points may be considered:

- **Not all data has the same value.** And, as such, the information may be handled and protected differently. Organizations must determine the value of the different types of information in their environment before they can plan for the appropriate levels of protection.
- **Know where the critical data resides.** In today's business environment, this is normally the company's information systems infrastructure. Because each piece of information may require different levels of protection, identifying where each is located enables an organization to establish an integrated security solution. This approach also provides significant cost benefits, as the company does not need to spend more on protecting data than the data itself is worth. Protection solutions must be based on the most valuable information assets. The network environment also presents additional challenges to protecting information.
- **Develop an access control methodology.** Information that is inadvertently damaged disclosed or copied without the knowledge of the owner may render the data useless. To guard against this, organizations must establish some type of access control methodology. For important data, this access control (and the associated auditing) should extend to the file level. Such access control extends from the host to the network. There are many types of solutions designed to provide this protected access.
- **Protect information stored on media.** Employees can cause considerable damage by walking out the door with information on 3 ½-inch floppy disks or CD-ROMS. In addition, companies should control magnetic media to reduce the loss of software (both application and operating system). And finally, when migrating from one platform to another, the status of all hard drives, and the associated data, should be controlled.
- **Review hardcopy output.** The hardcopy output of employees' daily work should also be reviewed. Although strategic plans in their final forms may be adequately protected, what measures are used safeguard all drafts and working papers? What information is regularly placed in the recycle or trash containers without thought to its value?

Based on this limited discussion, it is clear that much of the information that is so essential to successful business operations could be destructive if it is misused by employees, or should fall into the wrong hands. The exposure of this information to unauthorized individuals is greatly increased when companies connect their computers to other networks and the Internet. Computer systems and networks are inherently prone to data theft, loss, damage or destruction. Protecting such information must be done holistically, providing the organization with the appropriate level of security at a cost that is acceptable to the business.

WHAT ARE THE PRINCIPLES OF INFORMATION SECURITY?

The security objective is supported by eight core principles – accountability, awareness, multidisciplinary, cost effectiveness, integration, reassessment, timeliness, and societal factors. Each core principle is briefly discussed below.

Accountability—Responsibility and accountability must be explicit:

Security of information requires an express and timely allotment of responsibility and accountability among data owners, process owners, technology providers, and users. This accountability should be formalized and communicated.

Awareness—Awareness of risks and security initiatives must be disseminated:

Security measures are only effective if all involved are aware of their proper functioning and of the risks they address.

Multidisciplinary—security must be addressed taking into consideration both technological and non-technological issues:
Security is more than just technology. It also covers administrative, organizational, operational, and legal issues. Accordingly, technical standards should be developed with and, be reinforced by, codes of practice; audit; legislative, legal, and regulatory requirements; and awareness, education, and training.

Cost Effectiveness-Security must be cost-effective:
Different levels and types of security may be required to address the risks to information. Security levels and associated costs must be compatible with the value of the information.

Integration-Security must be coordinated and integrated:
Measures, practices, and procedures for the security of information should be coordinated and integrated with each other and with other measures, practices, and procedures of the organization, and third parties on whom the organization's business processes depend, so as to create a coherent system of security. This requires that all levels of the information cycle-gathering, processing, storing, sharing, transmitting, retrieving, and deleting-are covered.

Reassessment-Security must be reassessed periodically:
The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.

Timeliness—security procedures must provide for monitoring and timely response:
Organizations must establish procedures to monitor and respond to real or attempted breaches in security in a timely manner in proportion with the risk. The increasingly interconnected real-time and transferred nature of information and the potential for damage to occur rapidly require that organizations react rapidly.

Societal Factors—Ethics must be promoted by respecting the rights and interests of others:
Information and the security of information should be provided and used in such a manner that the rights and interests of others are respected and that the level of security must be consistent with the use and flow of information that is the hallmark of a democratic society.

PROTECTING COMPUTER-HELD INFORMATION
In the above section we discussed that not all information is equal and that some information requires greater protection than other information. Making the very broad assumption that all of an organization's valuable information is held electronically on a computer, we can now consider how this information should be protected.

Prior to discussing the details of how to protect the information, we need to define a few basic ground rules that must be addressed sequentially:

- **Rule #1:** We need to know what the information is and where it is located.
- **Rule #2:** we need know the value of the information held and how difficult it would be to recreate if it were damaged or lost.
- **Rule #3:** We need to know who is authorized to access the information and what they are permitted to do with the information.
- **Rule #4:** We need to know how quickly information needs to be made available if it become unavailable for whatever reason (loss, unauthorized modification, etc.)

These four rules are appears to be simple. For most organizations, providing answers to permit the design and implementation of any information protection is very tough.

There are two basic types of protection that or organization can use: Preventative and Restorative.

Preventative Information Protection: This type of protection is based on use of security controls. Information security controls are generally grouped into three types of control: Physical, Logical, and Administrative. Organizations require all three types of controls. The organization's Information Security Policy through the associated Information Security Standards documentation mandates use of these controls.

Here are some examples of each type of control:

- **Physical:** Doors, Locks, Guards, Floppy Disk Access Locks. Cables locking systems to desks/walls, CCTV. Paper shredders. Fire Suppression Systems
- **Logical (Technical):** Passwords, File Permissions. Access Control Lists. Account Privileges, Power Protection Systems
- **Administrative:** Security Awareness. User Account Revocation Policy etc

Restorative Information Protection: Security events that damage information will happen. If an organization cannot recover or recreate critical information in an acceptable time period, the organization will suffer and possibly have to go out of business.

Planning and operating an effective and timely information backup and recovery program is vital to an operation. Information backup does not simply involve backing up "just the valuable information". But it frequently also means backing up the system as well, since the information may need services that the system provides to make the information usable.

The key requirement of any restorative information protection plan is that the information can be recovered. This is frequently an issue that many organizations fail to properly address. There is a common belief that if the backup program claimed it wrote the information to the backup media, it can be recovered from the backup media. However, there are many variables that can prove that belief wrong.

Here are a few questions any restorative information protection program must address:

- Has the recovery process been tested recently?
- How long did it take?
- How much productivity was lost?
- Did everything go according to plan?
- How much extra time was needed to input the data changes since the last backup?

WHAT IS THE BEST APPROACH TO IMPLEMENT INFORMATION SECURITY?

To meet the security objective, and develop and maintain adequate controls in compliance with generally accepted core principles, an ongoing and integrated approach is necessary. Executive management and especially chief executive officer support is essential for the successful development, design, implementation, and monitoring of security controls.

Security Policies: Every organization should have a security policy that defines acceptable behaviors and the reaction of the organization when such behaviors are violated. Security policies are not unique and might differ from organization to organization. The electronic trading, viruses affecting organization's security documents and the misuse of credit cards have increased and this has augmented the need for security management. These commercial, competitive and legislative pressures require the implementation of proper security policies.

Policy Development: The security objective and core principles provide a framework for the first critical step for any organization-developing a security policy. The security policy 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 an organization. The information security policy should describe:

- The importance of information security to the organization;
- A statement from the chief executive officer in support of the goals and principles of effective information security:
- Specific statements indicating minimum standards and compliance requirements for specific areas:
  a. Assets classification;
  b. Data security;
  c. Personnel security;
  d. Physical, logical, and environmental security;
  e. Communications security;
  f. Legal, regulatory, and contractual requirements;
  g. System development and maintenance life cycle requirements;
  h. Business continuity planning;
  i. Security awareness, training, and education;
  j. Security breach detection and reporting requirements; and
  k. Violation enforcement provisions.
  l. Definitions of responsibilities and accountabilities for information security, with appropriate separation of duties;
  m. Particular information system or issue specific areas; and
  n. Reporting responsibilities and procedures.

Role and Responsibilities: For security to be effective, it is imperative that individual roles, responsibilities, and authority are clearly communicated and understood by all. Since every organization will have its own unique needs, it is not possible to provide a generic approach. Organizations must assign security-related functions in the appropriate manner to nominated employees. Responsibilities to consider include:

Executive Management-assigned overall responsibility for the security of information.

Information Systems Security Professionals—responsible for the 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 as well as 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 systems;

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: Once a policy has been approved by the governing body of the organization and related roles and responsibilities assigned, it is necessary to develop a security and control framework. This consists of standards, measures, practices, and procedures within which individual systems are then introduced and maintained.

When designing new or improved standards, measures, practices and procedures for the security of information systems, it is important to consider individual business requirements and the risks related to the particular system in order to identify the specific security requirements. Assessments of the risks must include both business and technical risks and the analysis of control objectives, standards, and techniques needed to provide an integrated control framework.

The process concludes with the design of an integrated security system that is compatible with the needs of the organization, given technical and cost constraints.

Implementation: Once the design of the security standards, measures, practices and procedures has been approved, the solution should be implemented on a timely basis, and then maintained. The security standards, measures, practices, and procedures will cover a number of subject areas including:

1. *Managerial controls*, such as span of control, separation of duties, background checks, and personnel awareness, training, and education to ensure that personnel act appropriately to prevent, detect, or correct problems.
2. *Identification and authentication controls* to establish accountability and to prevent unauthorized persons from gaining access to the systems through, for example, passwords or smart tokens;
3. *Logical access controls* to establish who or what has access to a specific type of information resources and the type of access permitted, such as read, write, update, or delete;
4. *Accountability controls* through management audit trails that maintain a record of all user and system activity;
5. *Cryptography Controls* over information transmitted and stored to ensure confidentiality, authenticity, integrity, and non-repudiation;
6. *Systems development life cycle process controls* to ensure that security is considered as an integral part of the process and explicitly considered during each phase of the process;
7. *Physical and environmental controls* (encompassing physical access, fire detection and prevention, air-conditioning and power supply continuity, structural soundness, and the physical security of data transmission lines) to ensure that adequate measures are taken against threats emanating from the physical environment;
8. *Computer support and operations controls* to ensure that these routine but critical activities (user support, software support, change management, configuration management, media controls, backups, documentation, and maintenance) enhance the overall level of security; and
9. *Business continuity planning controls* to ensure that an organization can prevent interruptions, and recover and resume processing in the event of a partial or total interruption to information systems availability.

Monitoring: Information systems are subject to a wide range of disruptive incidents of varying degrees of intensity. The business processes that rely on these systems and the environment, in which both these systems and processes operate, are also continually subject to change and new risks.

Preventive measures may not always be feasible or cost-effective to minimize loss, disclosure, damage, or disruption. Hence, monitoring measures need to be established to detect and ensure correction of security breaches, such that all actual and suspected breaches are promptly identified, investigated, and acted upon. This will also ensure ongoing compliance with policy, standards, and minimum acceptable security practices.

The immediate benefit of instituting monitoring measures and procedures over systems, processes, and their environment as to promptly identify damage and expedite recovery. The most important consequential benefit as that it increases the ability to prevent future damage and inconvenience. Actions that may result from monitoring practices are:

- Disciplinary or corrective actions.
- Minimization and recovery of losses.

- Refinement of security levels.
- Changes to policy or standards.
- Changes to design and implementation of security.
- Initiation of reassessment programs, including root cause and pattern analysis
- Initiation of intelligent monitoring systems with interactive feedback; and
- Initiation of network or system penetration studies.

Awareness, training, and Education: People are often the weakest link in securing information. Awareness of the need to protect information, training in the skills needed to operate them securely, and education in security measures and practices are of critical importance for the success of an organization's security program.

Security policy should be a broad statement that guides individuals and departments as they work to achieve certain goals. All the employees should aware of the security policies and its importance should be informed to all the employees on a regular basis. Security awareness is raised in a number of ways including.

- posting the security policies on the notice board or in the areas which are more frequently visited by employees
- training to all the staffs
- Non-disclosure statements signed by the employee
- Company newsletter
- Visible enforcement of security rules
- Periodic audits
- Conduct fake security incidents to improve security procedures

The following are the responsibilities of the 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 a good physical security of resources is maintained.
- Non-disclosure of access door lock combinations and questioning unfamiliar people

The overriding benefits of awareness, training, and education, are in improving employee behavior and attitudes towards information security and in increasing the ability to hold employees accountable for their actions. Raising the collective awareness level of the organization regarding security matters can be achieved through a variety of training methods-videos, newsletters, posters, briefings, etc. to be effective, the campaign must be creative and frequently changed.

INFORMATION SECURITY POLICY STATEMENT EXAMPLE

The purpose of the Information Security Policy is to protect the organization's information assets from all types of threats, whether internal or external, deliberate, or accidental. Information systems security is critical to the organization's survival.

It is the Policy of the organization to ensure that:

- Assets will be classified as to the level of protection required;
- Information will be protected against unauthorized access;
- Confidentiality of information will be assured;
- Integrity of information will be maintained;
- Personnel security requirements will be met;
- Physical, logical, and environment security (including communications security) will be maintained;

- Legal, regulatory, and contractual requirements will be met;
- Systems development and maintenance will be performed using a life cycle methodology;
- Business continuity plans will be produced, maintained, and tested.
- Information security awareness training will be provided to all staff;
- All breaches of information systems security, actual or suspected, will be reported to, and promptly investigated by Information Systems Security;
- Violations of Information Security Policy will result in penalties or sanctions;
- Standards, practices, and procedures will be produced, and measures implemented to support the Information Security Policy. These may include, but are not limited to, virus protection, passwords, and encryption.
- Business requirements for the availability of information and information systems will be met.
- The roles and responsibilities regarding information security are defined for:
  Executive management
  Information systems security professionals
  Data owners
  Process owners
  Technology providers
  Users
  Information systems auditors
- The Information Systems Security function has direct responsibility for maintaining the Information Security Policy and providing guidance and advice on its implementation.
- All managers are directly responsible for implementing the Information Security Policy within their areas of responsibility, and for adherence by their staff.
- It is the responsibility of each employee to adhere to the Information Security Policy.

ROLE OF A SECURITY ADMINISTRATOR

A security administrator is a person who is solely responsible for controlling and coordinating the activities belongs to all security aspects of the organization.

- A security administrator attempts to ensure that the facilities in which systems are developed, implemented, maintained and operated are safe from threats that affect the continuity of installation and or result in loss of security.
- The security administrator sets policy, subject to board approval.
- He also investigates, monitors, advise employees counsels management on matters pertaining to security.
- The security administrator is responsible for establishing the minimal fixed requirements for classification of information based on the physical, procedural, and logical security elements. The needs to protect these securities are also stressed; he assigns responsibilities to job classifications and formulates what to be done in case of exceptions.
- The security administrator guides other information security administrators and users on the selection and application of security measures, he trains them of how to mark and handle processes, train security coordinators, select software security packages and solve problems
- The security administrator also does the following
  Investigates all security violations
  Advises senior management on matters of information resource control.
  Consults on matters of information security
- A security administrator also has the responsibility of conducting a security program, which is a series of ongoing, regular, periodic evaluations of the facilities available.
- A security administrator has to consider an extensive list of possible threats to the organizations, prepare an inventory of assets evaluate the existing controls, implement new controls etc.

The security administrator requires the assistance of many individuals because of their expertise in that particular field. The auditor should see to that these steps are performed on a regular basis, the

results of the reviews are analyzed and documented, and advises the management on appropriate action in light of the results.

Security committee: End users, executive management, security administration personnel, IS personnel and legal counsel members should be an integral part of the security committee and discuss the policies and procedures regarding security periodically. They should draft methods that would efficiently follow the practices pertaining to security. The meeting dates, issues to be taken up, security topics to be discussed in the meeting are decided in advance and should be intimated to members to the security committee. There should be predefined procedures with respect to the committee and the committee should adhere to these steps to ensure the proper functioning of the committee.

KEY DEFINITIONS

Availability means the characteristic of data, information systems being accessible and useable on a timely basis in the required manner. Communications is the transmission and reception of signals and includes both voice and data communications.

Confidentiality means the characteristic of data and information being disclosed only to authorized persons, entities, and processes at authorized times and in an authorized manner.

Cyberspace means the global information and communications network where time, distance, and space are not a limitation.

Data means a representation of facts, concepts, or instructions, in a formalized manner suitable for communication, interpretation, or processing by human beings or by automatic means.

Information is the meaning assigned to data by means of conventions applied to that data.

Information Systems means the computers, communications facilities, computer and communications networks, and data and information that may be recorded, processed, stored, shared, transmitted, or retrieved by them, including programs, specifications, and procedures for their operation, use, and maintenance.

Information Systems Auditor is an auditor-either internal or external-who possesses the knowledge, skill, and abilities to review and evaluate the development, maintenance, and operation of components of information systems.

Integrity means the characteristics 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.

CHAPTER 19
Use of Simple CASE Tools, Analysis of Financial Statements using Digital Technology

INTRODUCTION

CASE provides the software engineer with the ability to automate manual activities and to improve engineering insight. Like computer-aided engineering and design tools that are used by engineers in other disciplines, CASE tools help to ensure that quality is designed in before the product is built.

WHAT ARE CASE TOOLS?

CASE stands for 'Computer Aided Software Engineering'. CASE TOOLS are automated software tools.

Software Engineering is concerned with creation of Systems Software, which are produced by teams of people using sound Engineering principles. They use computing techniques and the aim is to produce automated tools to solve specific problems of users in the domain of their function such as Finance, Production, and Sales etc and also to develop and produce software for such applications.

All dimensions of software engineering are coming together to form integrated environments. The four key components comprising these environments are

1. *Analysis Dimension* consisting of planning systems, defining requirements and designing systems.
2. *Development Dimension* consisting of traditional Programming Development tools like Editors, Compilers, Debuggers, Code and Application Generators.
3. *Management Dimension* provides methods and tools needed to manage and control projects.
4. *Support Dimension* comprising all tools and techniques needed to sustain and evolve existing software systems.

There are a number of software tools available today, which support software engineers. These automated tools enable to improve productivity in the area in software development and specific application software areas.

Evolution of CASE tools?

CASE covers computer-based procedures, techniques, and tools, which can be used to develop, maintain and reengineer software. CASE began to be recognized in the late 1980s with the advent of integrated project support environments, integration frame works, convergence of existing system maintenance and new development, object oriented design approaches, and the need to control software engineering process. In the middle of 90s, CASE tool vendors began developing tools for object oriented development, client-server development, configuration management, framework, repository and testing tools and interfacing with the tools of other vendors and ensuring portability of their products across multiple platforms.

The 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 where team of software engineers work together to produce software.

Case classification

CASE technology allows different types of tools to be assessed and compared. It also provides a conceptual basis of understanding.

There are three categories of CASE tools.

1. Tools that support individual process tasks such as checking the consistency of a design, compiling a program, comparing test results and so on.
2. Work benches to support process phases such as specification, design etc. they consist of sets of tools with variable degree of integration.
3. Environments support for all or part of software process. Includes several different work benches which are integrated in some way.

The tables given below lists a number of different types of CASE tools and gives specific examples of each tool.

Tool type	Example
Management tools	PERT tools, estimation tools
Editing tools	Text editors, diagram editors, word processors
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 systems, program restructuring systems

Integrated case tools:

Specialized Case tools can be combined together to provide a wider support to software process activities. An effective integration for framework makes evolution possible as new systems are added without disturbing the existing systems. In system engineering environment, there are five different levels of integration of CASE tools which are possible.

1. Platform integration: Tools run on the same hardware/operating system platform.
2. Data integration: Tools operate using a shared data model.
3. Presentation integration: Tools offer a common user interface.
4. Control integration: Tools may activate and control the operation of other tools.
5. Process integration: guided by a process model.

Let us examine each of these in detail.

1. Platform integration: Platform integration means that the tools or work benches to be implemented to run on the same platform where platform means either single computer/operating system or a network of systems.
2. Data integration: Data integration is the process of exchange of data by CASE tools. The result from one tool can be passed on as input to another tool.

   There are a number of different levels of data integration:
   a. Shared files: all tools recognize a single file format. The most general purpose shareable file format is where files are made of lines of characters.
   b. Shared data structures: The tools make use of shared data structures which usually include program or design language information.
   c. Shared repository: The 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 the tools.
3. Presentation Integration: Presentation or user interface integration means that the tools in the system use a common style and a set of common standards for user interaction.

   There are three different levels of presentation integration.
   a. Window system integration: Tools which are integrated at this level use the same underlying window system and present a common interface for window manipulation commands.
   b. Tools which are integrated at this level use the same form of commands for comparable functions.
   c. Interaction integration: This is related with a direct manipulation interface where the user 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. The tool can also call the sources of another tool in the system.

5. Process integration: Process Integration means that the CASE system has embedded knowledge about the process activities, their phasing, their constraints and the tools needed to support their activities. The CASE system participates in the scheduling of these activities and in checking that the required activity reference is maintained.

   Process integration requires that the CASE system maintains a mould of the software process and uses this mould to drive the process activities. In a sense, activities and deliverables are identified, a coordination strategy defined and the tools required to support activities are specified. All of this is embedded in the mould and a process interpreter then extracts this mould to drive the software process.

CASE WORK BENCHES

CASE work benches are available to support most software process activities. There are many types of CASE workbenches.

1. Programming workbench: Programming work bench is made up of a set of tools to support the process of program development. Some of these tools which are part of a programming workbench are:
   a. Language compiler: Translates host programs to object code. As part of a translation process, an abstract syntax tree and a symbol table is created.
   b. Structured editor: Incorporates embedded programming language knowledge and edits the syntax representation of the program in the AST rather than its source code text.
   c. Linker: Links the object code program with components which have already been compiled.
   d. Loader: Loads the executable program into the computer memory prior to execution.
   e. Cross reference: Produces a cross reference listing showing where all program names are declared and used.
   f. Pretty printer: Scans the AST and prints the source program according to embedded formatting rules.
   g. Static analyser: Analyses the source code to discover anomalies such as uninitialized variables, unreachable code, uncalled functions and procedures etc.
   h. Dynamic analyser: Produces a source code listing annotated with the number of times each statement was executed when the program was run. It may also generate information on program branches and loops and statistics of processor usage.
   i. Interactive debugger: Allows the user to control the execution sequence and view the program state as execution progresses.

2. 4GL Work benches: 4GL work benches are geared towards producing interactive application which rely on extracting information from the organizational data base, presenting it to end users on their terminal or work stations and then updating the database with changes made by users. The user interface usually consists of a set of standard forms or a spread-sheet. The tools which may be included in a work bench are:

   a. A database query language such as SQL which may either be input directly or generated automatically from forms filled in by end users.
   b. A form design tool which is used to create forms for data input and display.
   c. A spread-sheet which is used for the analysis and manipulation of numeric information.
   d. A report generator which is used to define and create reports from information in the database.

3. Analysis and design work benches: Analysis and design work benches are designed to support the analysis and design stages of the software process where models of the system are created.

   a. Diagram editors to create data flow diagrams, structured charts, entity relationship diagram and so on.
   b. Design analysis and checking tools which process the design and then submit report on errors and anomalies. These are integrated with editing system so that user errors are trapped at an early stage in the process.
   c. Repository query languages which allow the designer to find the designs and associate design information in the repository.
   d. A data dictionary which maintains information about the entities used in a system design.
   e. Report definition and generation tools which take information from the central store and automatically generate system documentation.
   f. Forms definition tools which allow screen and document formats to be specified.
   g. Import-export facilities which allow the interchange of information from the central repository with other development tools.
   h. Code generators which generate code or code skeletons automatically from the design captured in the central store.

4. Testing workbenches: Testing workbenches are open systems which evolve to suit the needs of the system being tested.

   The tools which might be included in a testing work bench are:
   a. Test manager: Manages the running and reporting of program tests. This involves keeping track of test data, expected results, program facilities tested and so on.
   b. Test data generator: Generates test data for the program to be tested. This may be accomplished by selecting data from a database or by using patterns to generate random data of the correct form.
   c. Oracle: Generates predictions of expected results.
   d. Files compactor: Compares the result of program tests with previous test results and reports differences between them.
   e. Report generator: Provides report definition and generation facilities for test results.
   f. Dynamic analyser: Add code to a program to count the number of times each statement has been executed.
   g. Simulators: Different kinds of simulators such as Target Simulators. User Interface simulators. I/O simulators are available for simulation.

5. Meta CASE workbenches: Meta case workbenches are CASE tools which are used to generate other CASE tools.

   They are usually based on a description of the rules and notations of design or analysis methods.

There are five different aspects which are to be considered in Meta-case work bench
   a. A data model for data capture and output generation.
   b. A frame model which defines the views of the data model to be generated. Each possible view of the data model is termed as frame. Links between frames which allows navigation from one representation to another are defined in this model.
   c. Diagrammatic notation for each diagram frame.
   d. Textual presentation for each text frame.

Typical components of a case work bench:

a. A diagram editing system that is used to create data flow diagrams, structure charts, entity relationship diagrams etc. it captures information about these entities and saves this information in a central repository.

b. Design analysis and checking facilities that process the design and correct errors. These are integrated with the editing system so that the users may be informed of errors during diagram creation.
c. Query language facilities that allows the user to browse the stored information and examine completed designs.
d. Data dictionary that maintains information about named entities in a system design.
e. Report generation tools that allow interchange of information from the central repository with other development tools.
f. Some system support skeleton code generation which generate code or code segments automatically from the design captured in the central store.

An example of CASE tool Set: As an illustration of the tools which might populate an environment for developing real-time software on a target microprocessor system, the following tools might be made available.

1. Host target communication software: This links the development computer to the computer on which the software is to execute, that is, the target machine.
2. Target machine simulation: These are used when target machine software is being developed so that it may be executed and tested on the host machine.
3. Cross-compilers: These are language processing systems which execute on the host machine and generate code for the target machine.
4. Testing and de-bugging tools: These might include test drivers, dynamic and static program analysers, and test output analysis programs. Debugging on the host of programs and executing on the target should be supported if possible.
5. Graphical design editors: These can be compared to those incorporated in CASE work benches but are tailored to support a real-time method.
6. Text processors: These support documentation development on the same machine as program development. This simplifies the task of producing and updating documentation as the system is developed
7. Project Management Tools: These software allow estimates of the time required for a project and the cost of the project to be made. Further more, they may provide facilities for generating management reports on the status of project at any time.

In addition to these tools, which are supportive of a particular application domain, the environment should provide a number of tools for configuration management, change control, version control and variant management.

CASE environment: A complete 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.

ANALYSIS OF FINANCIAL INFORMATION

Introduction: A computer can add value to the information and material work as they pass through different functional departments of an enterprise. It can also capture pertinent information and present it to the concerned person for the purpose of analysis and decision making.

Facilities are available in financial modules/packages to capture data in a secured way, store the data consistently and then enable analysis of the data captured for on going developments and further processing.

Various types of tools are available to store, process and output data in a secured manner. In such systems, there is no way of entering an illegal data from outside world. Every time a transaction takes place, a document is created and stamped with date and time. The terminal device signs the document and the user is compelled to leave his or her identification there too. If a transaction is legal but with error, a correction transaction must be generated. This too leaves its mark on the audit trail by generating a suitable records.

In financial Accounting costs, charges and profits are linked to the time period and cost/profit centre to which they belong rather than to a general fund. The purpose is to reveal the true value the company is gaining of whatever activity it is doing using its resources.

Checking the Data using Digital Techniques: Using digital techniques, entry of data is checked automatically at every stage. This checking is necessary to see whether information is dependable, whether the figure balances or whether transaction is legal. It also checks that the decision maker is authorised to make the choice. This data checking is done as per the standards of GAPP(Generally Accepted Accounting Principles).

An ideal computerized accounting system is able to recreate an unbroken audit trail for each and every transaction to the Balance Sheet and profit and loss accounts of the company.

Generally in an accounting system, a natural class of accounts will be in place. There is also the General Ledger with Accounts Payable and Accounts Receivable sub-ledgers which are integrated with General Ledger. The Cash Management Module is concerned with bank balances and cash on a daily basis.

The general ledger is the source from which external accounting documents, the balance sheet, profit and loss statement are built. Because this information is to be audited, it must be supported by audit trails that show how each summary total is computed.

Controlling depends on detailed record keeping in which individual parameters retain their identification, date, resources and identification of users who work on them.

The statements from the journal, the accounts, the trail balance, and the final statements provide fundamental monitoring of business directions in terms of movements and progress, strategic goals and operating tactics.

The data available in these documents can be subsequently analysed. The general ledger and sub-ledger provide this central source. From the source of General Ledger, it is possible to extract and analyse ratios such as cash flow proportions, work load proportions etc. liquidity can also to be analysed with General Ledger accounting by looking at projected cash disbursement and receipts in the short and medium periods.

FINANCIAL ANALYSIS

Planning the Finance: The financial planning for an Enterprise is carried out by suitably examining and analysing the financial data centrally available. Based on these data, corrective actions are taken on future processes for onward progress and development.

Ratio Analysis: One important benefit of having an up-to-date accounting system with a flexible reporting facility on a powerful computer is the speed with which complex business calculations can be provided with the information necessary to ensure that they are valid. A frequently used outcome of business calculations is the ratio a comparison between two numerical values obtained by dividing one by the other.

A ratio that compares one production period with another can be a useful indicator to guide internal management. The financial position of the company can be compared with that of a rival company by means of one or more ratios. Ratios between individual company performance and consolidated financial statement amounts can be used to explain or amplify the annual report.
Facilities are available to define the same mathematical procedure for all these ratios and calculations, but the actual variables and data depend on the purpose and the version number of the ratio calculation specified when the result is called. Suppose the ratio calculations are defined in two stages. The specifications required are

- Specifying where information is to come
- Specifying how the information is to take part in the calculation

There are certain financial ratios which help financial personnel make better use of financial information in planning and control.

These ratios can be broadly classified into three main areas. They are

Profitability.
Liquidity.
Efficiency or activity.

Let us examine these in detail.

1. profitability ratios:
   a. gross profit as a Percentage of net capital employed: This is calculated using the formula:
      Gross Profit*100/Net Capital Employed
      If the figures over a period of 5 years are 6.6%, 6.7%, 6.7%, 6.8%, 6.8% then these are acceptable, but figures such as 6.0%,7.2%,5.8%,6.3%,7.0% are not acceptable.
   b. Net Profit as a percentage of the net capital employed. This is calculated using the formula:
      Net Profit*100/Net Capital Employed.
   c. Gross Profit as a percentage of Sales: This is calculated using the formula:
      Gross Profit*100/Sales.
   d. Net profit as a percent of Sales: This uses the formula:
      Net Profit*100/Sales.

2. Liquidity Ratios:

These ratios are concerned with an undertaking's ability to pay in a short and medium time frame. This is only a trend figure over a period of time say 5 years.

1. Current ratios: This is represented by the ratio
   Current Assets/Current Liabilities.
   The current liabilities are always indicated as 1.
   It is important to know average value for the sector and the trend for this ratio.

2. Quick Ratio: This is given by quick assets as a ratio of the current liabilities. The quick assets are those that can be readily turned into cash.
   a. Long term solvency ratios, gearing and interest cover: The greater the borrowing a proportion of total long term financing, the higher the risk of business failure.
      The gearing ratio has to be less than the average in the business sector.
      Interest cover is calculated by dividing profit before interest by the interest charged.

   b. Efficiency Ratio or Activity Ratios: Efficiency ratios indicate how effectively the inventory, creditors, Debtors of the organization are managed. This is related to working capital.

   Rate of Inventory turnover: Rough average inventory holding is given by

      (Opening Inventory + Closing inventory)/2.

      It is necessary to look at the trend over the last 5 years and also the average for the sector.

Speed of turnover of creditors: This indicates how many times the creditors are turned over for making payments. It is to be made sure that they are not paying their suppliers more quickly than they receive money from customers.

Speed of turnover of Debtors: This indicates that enable an enterprise to survive and successfully meet the operating targets.