

## PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

### QUESTIONS

#### Basic Concepts of Systems

1. (a) Write a note on deterministic and probabilistic systems  
(b) Define "Information". What are the characteristics of good or useful information?

#### Transaction Processing Systems

2. (a) Explain the coding in Accounting Information System (AIS) of Transaction Processing System (TPS).  
(b) Discuss in brief the transaction cycles which exist in all businesses?

#### Basic Concepts of MIS

3. (a) What is Management Information System? With the help of a figure explain the functions of MIS of an organisation.  
(b) What are the major constraints in operating a Management Information System?

#### Systems Approach and Decision Making

4. (a) Explain the role played by Financial Information System in making financial decisions.  
(b) Draw a schematic chart representing the flow of information for making financial decisions.

#### Decision Support and Executive Information Systems

5. (a) Describe Decision Support Systems (DSSs). What are their major components?  
(b) List out the software tools of Decision Support System.

#### Enabling Technologies

6. (a) Explain the characteristics of Client-Server technology.  
(b) Describe the various components of Client-Server architecture.

#### System Development Process

7. (a) Draw a context diagram for payroll processing.  
(b) Why should users be involved in the software development process?

#### Systems Design

8. (a) Distinguish between logical design and physical design.  
(b) Discuss briefly the guidelines based on which the printed and visual display outputs are designed.

#### System's Acquisition, Software Development and Testing

9. (a) Discuss some of the program design tools available for software development.
- (b) What basic features should be ascertained by the system analyst before purchasing packaged software?

#### Systems Implementation and Maintenance

10. (a) Discuss in brief operation evaluation of the new system.
- (b) Why is personnel training important for the success of systems implementation? What type of training should be imparted to system operators and users?

#### Design of Computerised Commercial Applications

11. (a) Write an overview of an Accounting Information System.
- (b) Draw a flow chart explaining the processes involved in a payroll application.

#### Enterprise Resource Planning: Redesigning Business

12. List out various steps involved in the implementation of a typical ERP package
13. List out various functions of Treasury Cash Management

#### Controls in EDP Set-up: General Controls

14. Explain the following:
  - (a) Access token
  - (b) Access control list
  - (c) Threats to operating system integrity.
15. What controls and procedures can be adopted to reduce threats from misuse of passwords?

#### Controls in EDP Set-up: Application Controls

16. What is a source document fraud? What controls can be used to prevent this type of frauds?
17. Explain the following input controls.
  - (a) Data coding controls
  - (b) Validation controls
  - (c) Input error correction
18. Briefly describe the various checks that could be performed during the validation run.

#### Detection of Computer Frauds

19. (a) "During computer processing the system might fail to detect erroneous input, improperly correct input errors, process erroneous input, or improperly distribute or

disclose output". Discuss the control procedure to detect and prevent these errors and the system review and the test of control procedures employed by the auditor.

- (b) What measures can be taken by the organization to prevent computer fraud?

#### Cyber Laws and Information Technology Act, 2000

20. Define some of the following terms as mentioned in Information Technology Act, 2000:

- (a) Computer System
- (b) Computer Network
- (c) Digital Signature
- (d) Secure System

21. Discuss various sections relating to suspension and revocation of digital signature certificate.

#### Audit of Information Systems

22. (a) Explain the purpose of using reprocessing technique and parallel simulation to the auditor.

- (b) Describe the major techniques of concurrent audit of information systems.

#### Information Security

23. (a) Briefly describe the role of awareness, training and education in implementing Information security.

- (b) Give examples of the information security controls.

#### Use of Simple Case Tools, Analysis of Financial Statements using Digital Technology

24. (a) What are CASE Tools? Explain the benefits of Computer Aided Software Engineering.

- (b) Write a short note on evolution of CASE tools.

25. What is a programming CASE work-bench? Give some tools, which are part of a programming work-bench.

#### SUGGESTED ANSWERS/HINTS

1. (a) 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 in 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.

The probabilistic system can be described in terms of probable behaviour, but 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.

- (b) Information is data that has been put into a meaningful and useful context. It is 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.”

The term “data” and “information” are often used interchangeably. However, the relation of data to information is that of raw material to finished product. Business decisions are generally based on the information. The management plays the part of converting the information into action through the process of decision-making.

Information flows are as important to the survival of a business as the flow of blood is to the life and survival of an individual. Information flow is important for good business decisions and it has been often said that a receipt of a good business is “90% information and 10% inspiration.”

Important characteristics of good or useful information are as follows:

- |                  |                 |                           |
|------------------|-----------------|---------------------------|
| (a) Timeliness   | (b) Purpose     | (c) Mode and Format       |
| (d) Redundancy   | (e) Rate        | (f) Frequency             |
| (g) Completeness | (h) Reliability | (i) Cost-benefit analysis |
| (j) Validity     | (k) Quality     |                           |

For details to above points, please refer to study material, Chapter-1, Section 1.5.1.

2. (a) For a transaction processing system to gather and process data efficiently, accounting data are often coded. AISs can use codes to identify accounting information uniquely, to compress data, to classify transactions in accounts, and to convey special meanings.

Four types of codes are generally used:

- (i) Mnemonic codes,
- (ii) Sequence codes,
- (iii) Block codes, and
- (iv) Group codes.

The choices among these codes and the way these codes are constructed are determined by:

- The code's use,
- The need for consistency,

- Considerations of design efficiency,
  - An allowance for growth, and
  - The desire to use standard codes throughout a company.
- (b) A transaction processing cycle organises transactions by an organisation's business processes. The nature and types of transaction processing cycles vary, depending on the information needs of a specific organisation. Nevertheless, most business organisations have in common, transactions that may be grouped according to four common cycles of business activity. These cycles exist in all types of business – both profit –seeking and not – for- profit.
- (a) Revenue cycle: Firms sell their finished goods to customers through this cycle. It involves processing cash sales, credit sales, and receipt of cash following a credit sale.
  - (b) Expenditure cycle: Events related to acquisition of goods and services from other entities in exchange for cash.
  - (c) Production cycle: Events related to the transformation of resources into goods and services. It involves the planning, scheduling, and control of the physical product through the manufacturing process.
  - (d) Finance cycle: Events related to the acquisition and management of capital funds, including cash. It might also include application systems concerned with cash management and control, debt management, and administration of employee benefit plans.

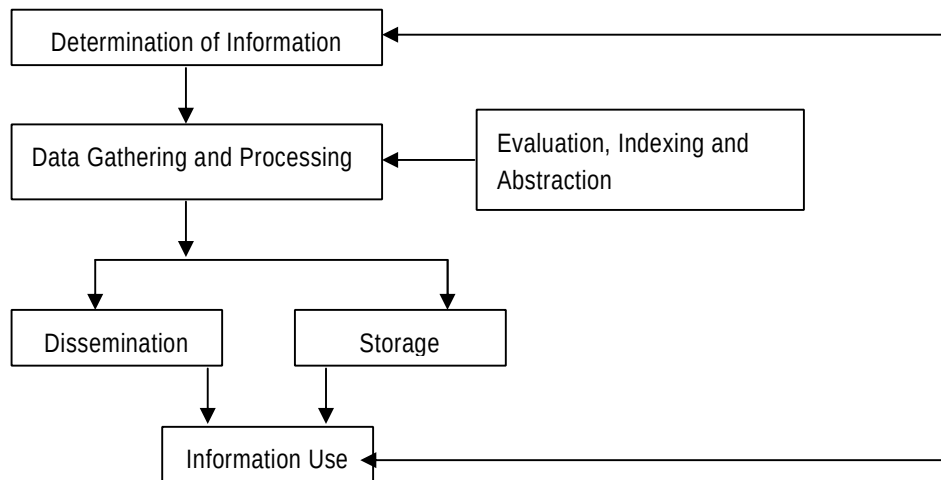
The transaction cycle model of an organisation includes a fifth cycle – the financial reporting cycle. It is not an operating cycle. It obtains accounting and operating data from other cycles and processes these data in such a manner that financial reports may be prepared.

3. (a) Management Information System: Information is critical to the success of any business organisation. Management Information System (MIS) is a computer based system which deals with the use, storage and retrieval of information in an organisation.

MIS is a "system of people, equipment, procedures, documents and communication that collects, validates, and operates on transformers, stores, retrieves and present data for use in various management activities such as planning, budgeting, accounting, controlling and various other processes.

Management Information Systems (MIS) are information systems typically computer-based, that are used within an organisation. An information system can be defined as "a system that collects and processes data (information) and provides it to managers at all levels who use it for decision making, planning, program implementation, and control." An information system is comprised of all the components that collect, manipulate, and disseminate data or information. It usually

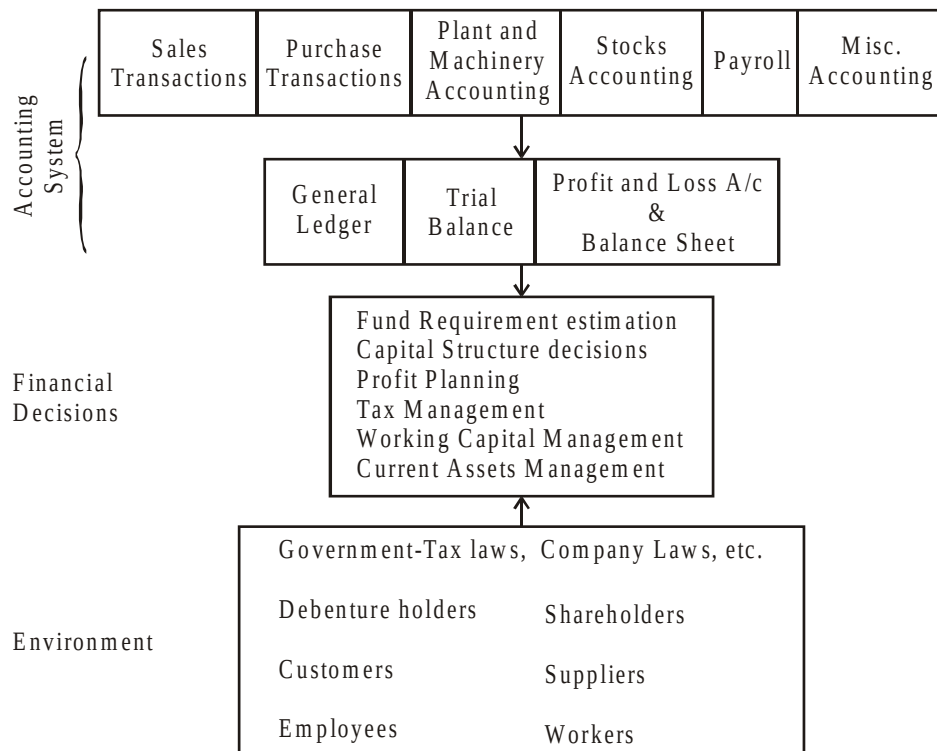
includes hardware, software, communications systems such as telephone lines, and the data itself. The activities involved include inputting data, processing of data into information, storage of data and information, and the production of outputs such as management reports. The functions of MIS can be shown with the help of the following diagram:



- (b) The major constraints which come in the way of operating a management information system are as follows:
- (i) Non-availability of experts, who can diagnose the objectives of the organisation and provide a desired direction for installing and operating system. This problem may be overcome by grooming internal staff. The grooming of staff should be preceded by proper selection and training.
  - (ii) Non-availability of standard MIS product. Experts usually face the problem of selecting the sub-system of MIS to be installed and operated upon.
  - (iii) Non-availability of cooperation from staff. Educating the staff may solve this problem. This task should be carried out by organising lectures, 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.
  - (iv) High turnover of experts in MIS. Turnover in fact arises due to several factors like pay packet; promotion chances; future prospects, behaviour 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.

- (v) Difficulty in quantifying the benefits of MIS, so that it can be easily comparable with cost. This raises questions by departmental managers about the utility of MIS.
4. (a) Financial information system plays an important role in making following financial decisions:
- (i) Estimation of requirements of funds: This is the very important and starting point of making financial decisions. A very careful estimation of funds and the time at which these funds are required is made in this stage. This can be done by forecasting all physical activities of the firm and translating them into monetary units.
  - (ii) Capital structure decisions: Decisions are to be taken to select an optimum mix of different sources of capital structure. There are many options available for procuring funds. Decision maker has to decide the ratio between debt and 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.
  - (iii) Capital budgeting decisions: Funds procured from various sources are required to be invested in different assets. With the help of capital budgeting, decision maker can determine feasibility of investment in long-term assets. This will help in attainment of financial objectives.
  - (iv) Profit planning: This part of profit planning is essential for the growth of the organisation. The decision maker has to make decision regarding profits and dividends.
  - (v) Tax management: Tax planning is aimed at reducing of outflow of cash resources by way of taxes so that the same may be effectively utilized for the benefit of business. The purpose of tax planning is to take full advantage of exemptions, deductions, concessions, rebates, allowances and other relief.
  - (vi) Working capital management: Working capital management is concerned with the 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.
  - (vii) Current assets management: Policy decisions are taken regarding various items of current assets. Credit policy determines the amount of sundry debtors at any point of time. Inventory policy is to be determined jointly between finance and production department.

- (b) The schematic chart representing flow of information for making financial decisions is given below:



5. (a) A Decision Support System (DSS) can be defined as 'a system that provides tools to managers to assist them in solving, semi-structured and unstructured problems.' It provides managers with a set of capabilities that enables them to generate the information required by them in making decisions. Thus, a DSS supports the human decision-making process, rather than providing a means to replace it.

A decision support system has four basic components:

- (i) The users
- (ii) Databases
- (iii) Planning languages
- (iv) Model base.

For details to above points, please refer to study material, Chapter 5, Section 5.3.



- (b) The tools of decision support include a variety of software supporting database query, modelling, data analysis and display. A comprehensive toolkit for DSS would include software supporting these application areas. Examples of software tools falling into these four categories are given in table below:

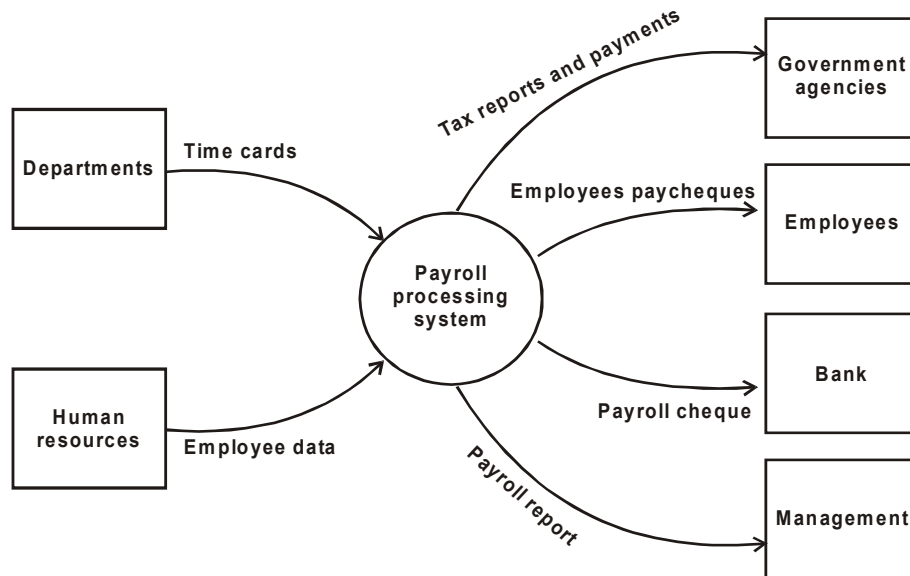
| Data based software | Model based software | Statistical software | Display based software |
|---------------------|----------------------|----------------------|------------------------|
| Dbase Plus          | IFPS                 | SAS                  | SASGRAPH               |
| Foxpro              | Lotus 1-2-3          | SPSS                 | TELLAGRAF              |
| Sysbase             | Multiplan            | Minitab              | ChartMaster            |
| R:base 7.6 / 5000   | Omnicalc             |                      |                        |
| SQL                 | Calc                 |                      |                        |
| MySQL               | Foresight            |                      |                        |

6. (a) The key characteristics of a client / server technology are:
- Client/server architecture consists of a client process and a server process that can be distinguished from each other.
  - The client portion and the server portions can operate on separate computer platforms.
  - Either the client platform or the server platform can be upgraded without having to upgrade the other platform.
  - The server is able to service multiple clients concurrently; in some client/server systems, clients can access multiple servers.
  - The client/server system includes some sort of networking capability.
  - A significant portion of the application logic resides at the client end.
  - Action is usually initiated at the client end, not the server end.
  - A user-friendly Graphical User Interface (GUI) generally resides at the client end.
  - A Structured Query Language (SQL) capability is characteristic of the majority of client/ server systems.

- (b) Various components of client–server architecture are briefly described below:
- (i) Clients: Clients, which are typically PCs, are the “users” of the services offered by the servers. There are three types of clients: (a) Non-Graphical User Interface (NGUI) clients, (b) GUI-clients, (c) Object –Oriented User Interface (OOUI) clients.
    - (a) Non-GUI clients include ATMs, Cell phones, fax machines and robots that require minimum amount of human interaction.
    - (b) GUI-clients are human interaction models usually involving objects / action models like the pull-down menus as in windows operating system.
    - (c) OOUI clients take GUI clients even further with expanded visual formats, multiple work places, and object interaction rather than application interaction. Windows 95 is a common OOUI-client.
  - (ii) Servers: Servers await requests from the client and regulate access to shared resources. There are four types of servers:
    - (a) File server: It shares files across a network by maintaining a shared library of documents, data and images.
    - (b) Database server: This has processing power to execute Structured Query Language (SQL) requests from clients.
    - (c) Transaction server: It executes a series of SQL commands, an Online Transaction Processing program (OLTP) as opposed to database servers, which respond to a single client command.
    - (d) Web server: This allows clients and servers to communicate with a universal language called HTTP.
  - (iii) Middleware: The network system implemented within the client/server technology is commonly called by the computer industry as middleware. It is the distributed software that is needed to allow clients and servers to interact. 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.
  - (iv) Fat-client or Fat-server: Fat client or fat-servers are popular terms which serve as vivid description of the type of client/server system 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 minimise the processing done by clients. Examples of fat –server are groupware and web server. Visually fat-clients are referred to as 2-tier system and fat-servers referred to as 3-tier systems.

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

7. (a) The context diagram for payroll processing is given below:



- (b) Involving users in the development process provides valuable feedback and ensures that the users themselves understand the system's limitations and capabilities. Specifically, it enables users to share in the responsibility for the success or failure of the system developed for them. In addition, involving users secures their aid in detecting missing, unnecessary, or awkward system features and in pointing out errors in procedures, input and output specifications, data stores and other design features. Most importantly, user involvement often leads to productive changes in the specifications, thus preventing problems later in the development process.

8. (a) The differences between the logical design and physical design are:

- 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. Data and procedures are linked together to produce a working system.
- The physical design activity follows the logical design; the activity involves producing program software, files and a working system. Design specifications; instruct programmers about what the system should do. The programmers, in

turn, write the programs that accept input from users, process data, produce the reports, and store data in the files.

- (b) Following are the guidelines, which should be followed while preparing the printed and visual display outputs. It will not only make the analyst's job easier, but will also ensure that users will receive an understandable output.

Printed Outputs:

1. Reports and documents should be designed to read from left to right and top to bottom.
2. Most important items should be easiest to find.
3. Each printed reports should include the heading or title of the report, page number, date of preparation and column headings. The heading or title of the report orients the user to what it is they are reading. The title should be descriptive, yet concise. Each page should be numbered so that the user has an easy point of reference when discussing output with others or relocating important figures. The date of report preparation should be included on each print out. Sometimes this helps users to estimate the value of the output. Column headings serve to further orient the user as to the report contents.
4. Each data item must have a heading, which should be short and descriptive. Data items that are related to one another should be grouped together on the report.
5. Control breaks should be used in the report to help readability. There should be control breaks, summaries and other important information by boxing them off with special characters such as asterisks or extra space. This makes it easier to find critical information.
6. Sufficient margin should be made available 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.
7. The detail line for variable data should be defined by indicating whether each space is to be used for an alphabetic, special or numeric character.
8. The mock up reports should be reviewed by users and programmers for feasibility, usefulness, readability, understand ability and an aesthetic appeal.

Visual display outputs: Many of the principles of good design discussed for printed output also apply to output that is shown on work-stations or video display terminals. However, 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. Its layout will ease or impede its use. Designing a layout begins with verifying the characteristics of the display screen. These include:

- (i) Physical dimensions of the screen;
- (ii) Number of rows and columns of data that can be displayed;
- (iii) Degree of resolution (high, medium, low);
- (iv) Number of colours available (for example, monochrome, three colours, eight colours etc.);
- (v) Methods of highlighting (underline, bold, blinking, alternate intensities);
- (vi) Methods of intensity control (high / low; normal / inverse).

Visual display screens typically have 80 columns with 24 or 25 lines. Point-of-sale display and some portable computers have smaller dimensions. Screen design begins with the recognition that the screen is composed of different areas. Layout tools assist the analyst in specifying the contents of a single or multiple design formats.

It is helpful to divide the display screens into sections that are consistently used in the same way to present information, identifications and messages to the user. In designing output screens, we need areas for (i) headings and titles, (ii) content of the display, (iii) messages and instructions and (iv) sometimes explanations for the information in the report. The headings and titles are positioned as the top portion of the screen, messages and instructions at the bottom, and explanations if needed, on the right-hand side. If only a very small amount of information is to be presented, it can be placed in the centre of the screen or in the upper left quadrant. However, it is mainly a matter of preference of the concerned system analysts.

9. (a) Some of the several program design tools are discussed below:

- (i) 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. These flow charts 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.
- (ii) 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.

- (iii) 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 organisation charts, are useful for organising problems.
- (iv) 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.
- (v) Object oriented programming and design tools: These tools provide a means of enhancing programmer productivity and of reducing the application backlogs common in many organisations. Object oriented software design results in a model that describes 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.

For details to above points, please refer to study material, Chapter 9, Section 9.6.

- (b) The following features of package software may be ascertained before purchasing the same:
  - (i) What is the package designed to do?
  - (ii) How developed is the software package?
  - (iii) How is the package organised?
  - (iv) Is the package operable?
  - (v) Can the package operate on our hardware configuration?
  - (vi) Can the program provide the needed reports?
  - (vii) 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?

- (viii) 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 programme may, have to be executed several times, requiring more operator time and computer processing to complete the job.
  - (ix) 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.
  - (x) Will the package require modifications?
  - (xi) Can the package be modified if necessary?
  - (xii) What are the overall costs?
  - (xiii) Is comprehensive documentation available?
  - (xiv) Who will maintain the package?
  - (xv) What are the package constraints?
  - (xvi) Where is the package currently used?
  - (xvii) What is the primary language? How many languages the package support?
  - (xviii) What input/output techniques are utilised?
  - (xix) What are the required input/output formats?
  - (xx) How must input be organised?
  - (xxi) What kind of user training is provided or required?
10. (a) 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 as:
- Are all transactions processed on time?
  - Are all values computed accurately?
  - Is the system easy to work with and understand?
  - Is terminal response time within acceptable limits?
  - Are reports processed on time?
  - 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.

- (b) Importance of 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 professionals generally need some type of training. Often this is imparted through classes, which are organised by the vendor, and through hands-on learning techniques.

Training systems operators: Many systems depend on the computer-centre 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. Operator training must also involve the data entry personnel. If the system calls for the installation of new equipment, such as a new computer systems, special terminals or data-entry equipments, 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 recognise 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. Training also involves familiarization with run procedures, which involve working through the sequence of activities needed to use a new system on an on-going basis.

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 how to operate the equipment. User training must also instruct the 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. Training in data coding emphasises the methods to be followed in capturing data from transactions or preparing data for decision support activities. Users should be trained on data handling activities such as editing data, formulating inquiries (finding specific records or getting responses to questions) and deleting records of data. From time to time, users will have to prepare disks, load paper into printers, or change ribbons on printers. Some training time should be devoted to such system maintenance activities. If a micro computer or data entry system uses disks, users should be instructed in formatting and testing disks.

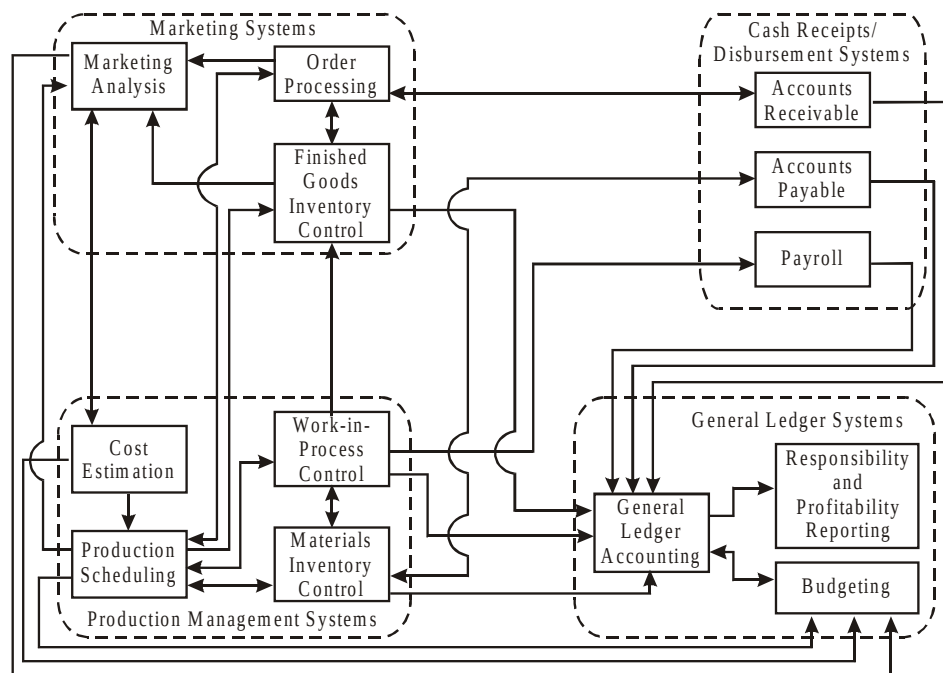
Training is often seen as a necessary evil by managers. While recognising its importance, many managers have to release employees from their regular job activities so that they can be trained. When managers are actively involved in



determining training needs, they are usually more supportive of training efforts. It is generally wise to have managers directly involved in evaluating the effectiveness of training activities because training deficiencies can translate into reduced user productivity level.

11. (a) A typical Accounting Information System can be divided into four separate areas:
  - (i) The general ledger systems, which include the general ledger, budgeting, and responsibility/profitability reporting.
  - (ii) The cash receipts/disbursements systems, which include the accounts payable, payroll and accounts receivable systems.
  - (iii) The production management systems, which include the materials inventory control, work-in-process control, cost estimation, and production scheduling systems.
  - (iv) The marketing systems, which include finished goods inventory control, order processing, and marketing analysis systems.

The flow lines between the various systems in the figure below illustrate interfaces between these systems. The arrows on the flow lines indicate the direction of the information flow from one system to another.



- (b) The flow chart drawn on the next page 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, reports and documents as 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. 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 in 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 rerun 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 cost code stored in master file indicates the nature of the account to which employee's gross pay is charged such as direct labour, indirect labour 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 pay slips and pay cheques for the current period are put on a magnetic 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 computed employee master file.

In run #4, the current period payroll master disk is used to produce pay cheques and pay slips.

In run #5, the current period payroll disk is sorted by job number.

In run # 6, the output file of run # 5 is used to update the old labour distribution file.

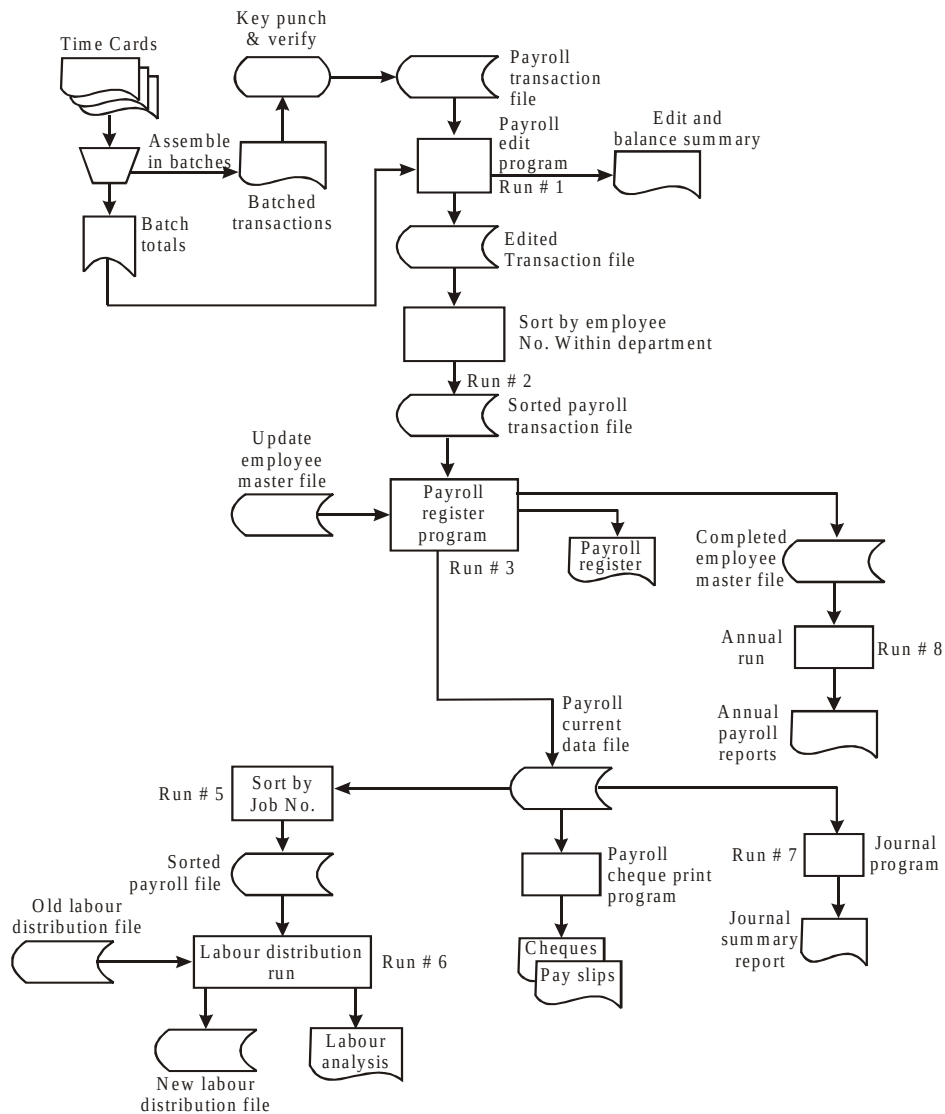
The cumulative values of various trades as at the end of last month are updated to as at the end of this month by means of the payroll file.

The 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.



12. Several steps are involved in the implementation of a typical ERP package. These are:
- (i) Identifying the needs for implementing an ERP package.
  - (ii) Evaluating the 'As Is' situation of the business i.e., to understand the strength and weakness prevailing under the existing circumstances.
  - (iii) Deciding the 'Would be' situation for the business i.e., the changes expected after the implementation of ERP.
  - (iv) Reengineering the business process to achieve the desired results in the existing processes.
  - (v) Evaluating the various available ERP packages to assess suitability.
  - (vi) Finalising of the most suitable ERP package for implementation.
  - (vii) Installing the required hardware and networks for the selected ERP package.
  - (viii) Finalising the Implementation consultants who will assist in implementation.
  - (ix) Implementing the ERP package.
13. In a Treasury cash management, the company's payment transactions are grouped into cash holdings, cash inflows and cash outflows. Cash Management provides following information:
- (i) Information on the sources and uses of funds to secure liquidity to meet payment obligations when they become due.
  - (ii) Monitors and Controls incoming and outgoing payment flows.
  - (iii) Supplies data required for managing short-term money market investment and borrowing.
  - (iv) Enables to know current cash position, short term cash management and medium and long term financial budgeting.
  - (v) Enables analysis of liquidity.
  - (vi) Helps in cash management decisions.
  - (vii) In bank accounting, helps in electronic banking and control functions for managing and monitoring of bank accounts.
  - (viii) The liquidity forecast function integrates anticipated payment flows from financial accounting, purchasing and sales to create a liquidity outlook from medium to long term.
  - (ix) Covers foreign currency holdings and foreign currency items.
14. (a) 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.

- (b) 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.
- (c) 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 program 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. These exposures come from three sources:

- (i) Privileged personnel who abuse their authority. Systems administrators and systems programmers require unlimited access to the operating system to perform maintenance and to recover from system failures. Such individuals may use this authority to access users' programs and data files.
  - (ii) Individuals both internal and external to the organisation who browse the operating system to identify and exploit security flaws.
  - (iii) An individual who intentionally (or accidentally) inserts a computer virus or other form of destructive program into the operating system.
15. The controls and procedures that can be adopted to reduce threats from misuse of passwords are:
- 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 user must be encouraged to use “Strong” passwords. Software's are 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.
  - The user should be educated about the use of strong passwords and the benefits of changing the passwords periodically.

- The user should be informed about possible traps that they may fall into if they reveal their login and passwords.
  - The authentication system must not allow re-entry of password more than 2-3 times in case the authentication fails.
16. Systems using physical source documents to initiate transactions are vulnerable to source document fraud. Source document fraud can be used to remove assets from the organisation. 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 had 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 organisation must implement control procedures over source documents to account for each document, as described below:
- (i) Use Prenumbered Source Documents: Source documents should come pre-numbered 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.
  - (ii) 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 authorised persons.
  - (iii) Periodically Audit Source Documents: Missing source documents should be identified by reconciling document sequence numbers. Periodically, the auditor should compare the numbers 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.
17. (a) 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 number are all examples of data codes. Three types of errors can corrupt a data code and cause processing errors: transcription, single transposition and multiple transposition. Check digit can be used to ensure integrity of the code in subsequent processing.
- (b) 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 CBIS in use, input validation may

occur at various points in the system. There are three levels of validation controls: field interrogation, transaction interrogation and file interrogation.

- (c) Input error correction: When errors are detected in a batch they must be corrected and the records 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: immediate correction; create an error file, and reject the entire batch.

For details to above points, please refer to study material, Chapter 14, Section 14.1.

- 18. The checks which could be performed during a validation run can be categorised as field checks and transaction checks. Various field checks have been described below:

- (i) Limit check: This is a basic test for data processing accuracy and may be applied to both the input and output data. The field is checked by the program against predefined limits to ensure that no input/output error has occurred or at least no input error exceeding certain pre-established limits has occurred.
- (ii) Picture check: Under this check, only certain characters are allowed in a data field. The computer can test the field to determine that no invalid characters are used.
- (iii) Valid code check: If there are a limited number of valid codes, the code being read may be checked against pre-determined transaction codes, or table to ensure that it is one of the valid codes.
- (iv) Check digit: It is an extra digit that is computed from the code itself and placed alongside it for subsequent checking. There are a number of check digit schemes. Module 11 check digit scheme has been empirically established as the best to detect transposition errors.
- (v) Arithmetic check: Arithmetic check is performed in different ways to validate the results of other computations or the value of selected data field.
- (vi) Valid combinations of fields: In addition to each of the individual fields being tested, combination of fields may be tested for validity.
- (vii) Cross check: It may be employed to verify fields appearing in different files to see that the results tally.
- (viii) Valid field size, sign and composition: If the code number should be specified number of digits in length, the computer may be programmed to test that the field size is as specified. If the sign of the field must always be positive or always negative, a test may be made to determine that the field does indeed contain a proper composition of characters.

Various transaction checks are given below:

- (i) Sequence checks are exercised to detect any missing transactions, off-serially numbered vouchers.
- (ii) Format completeness checks are used to check the presence and position of

all the fields in a transaction.

- (iii) Redundant data checks are employed to check the validity of codes with reference to the description.
- (iv) Checks may be incorporated to ensure that transactions pertain to the correct period.
- (v) Combination checks may be exercised on various fields of a file.
- (vi) Passwords may be issued to check entry of data by unauthorised persons in on-line systems.
- (vii) Probability checks are used to avoid unnecessary rejection of data as data can, on occasions, exceed normal values in a range due to purely random causes.

In addition to above checks, hash totals and batch totals can also be applied to ensure that all the transactions have been transcribed correctly.

19. (a) 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 system review and tests of control procedures which the auditor employs are given below. 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:

#### Types of Errors and Fraud

- Failure to detect incorrect, incomplete, or unauthorised 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.
- Competent 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 unauthorised code via analysis of program logic.
- Check accuracy and completeness of processing controls using test data.
- Monitor on-line processing systems for using concurrent audit techniques.
- Re-create selected reports to test for accuracy and completeness.

#### Compensating Controls

- Strong user controls.
- Effective source data controls.

- (b) Organisations must take every precaution to protect their information systems. A number of measures can significantly decrease the potential for fraud and any resulting losses.

- (i) **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. Organisations can take steps to increase employee integrity and reduce the likelihood of employees committing a fraud.
  - (ii) **Use Proper Hiring and Firing Practices:** A manager's most important responsibilities are 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 sabotage or copying confidential data before they leave.
  - (iii) **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.
  - (iv) **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.
20. (a) Some of the important terms as defined in the Information Technology Act, 2000 "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 programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;
- (b) "computer network" means the interconnection of one or more computers through-
- (i) the use of satellite, microwave, terrestrial line or other communication media; and
  - (ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;
- (c) "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;

- (d) "secure system" means computer hardware, software, and procedure that-
    - (a) are reasonably secure from unauthorised access and misuse;
    - (b) provide a reasonable level of reliability and correct operation;
    - (c) are reasonably suited to performing the intended functions; and
    - (d) adhere to generally accepted security procedures;
21. Suspension of digital signature certificate: Chapter VIII of the Act containing sections 35 to 39 lay down procedures relating to digital signature certification. The Certifying Authority may suspend such certificate if it is of the opinion that such a step needs 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 Certificate 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.
22. (a) The pre-processing technique and parallel simulation can be used by auditors to detect unauthorised program changes. The reprocessing technique 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.
- (b) Major techniques of concurrent audit of information systems are discussed below:
- (1) Integrated test facility technique: places a small set of fictitious records in the master file. Processing test transactions to update these dummy records will not affect the actual records. Because fictitious and actual records are processed together, employees remain unaware that this testing is taking place. The auditor compares processing and expected results in order to verify that the system and its controls are operating correctly.
  - (2) 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.

- (3) SCARF (System Control Audit File Review): 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. Periodically the auditor examines the information to identify any questionable transactions.
  - (4) Audit hooks: These are audit routines that flag suspicious transactions, for example, an Insurance Company determined that their policy holder systems was vulnerable to fraud each time a policy holder changed his name or address and subsequently withdrew money. Internal auditors of the company devised a system of audit hooks to tag records with a name or address change whenever a policy holder changed his name or address and then subsequently withdraw funds from the policy. When audit hooks are employed, auditors can be informed of questionable transactions as soon as they occur.
  - (5) Continuous and intermittent simulation (CIS): This 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, records the results and compares them with DBMS results. In case of discrepancies, the details are written into an audit log for subsequent investigation.
- 23 (a) 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 organisation's security program.

The overriding benefits of awareness, training, and education, are in improving employee behaviour and attitudes towards information security and in increasing the ability to hold employees accountable for their actions. Raising the collective awareness level of the organisation 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.

Training and communication are usually focused on security-related job skills and stimulate practices such as protecting the physical area and equipment (caring for media such as diskettes), protecting passwords, and reporting security violations. Advanced training may be needed for managers and specialised training necessary for system administrators and information systems auditors.

Education is more in-depth and typically targeted for information systems security professionals to gain expertise. It is normally achieved through external programs and should be regarded as part of career development.

(b) Information security controls are generally grouped into three types of control: Physical, Logical and Administrative. The examples of each type of control are as follows:

1. Physical: Doors, Locks, Guards, Floppy disk and magnetic disk access locks, Cables locking system to desks/walls, CCTV, Paper shredders and Fire Suppression Systems.
2. Logical (Technical): Passwords, File permissions, Access control lists, Account Privileges and Power protection Systems.
3. Administrative: Security Awareness, User Account Revocation Policy etc.

For details to above points, please refer to study material, Chapter-18, Section 18.4.

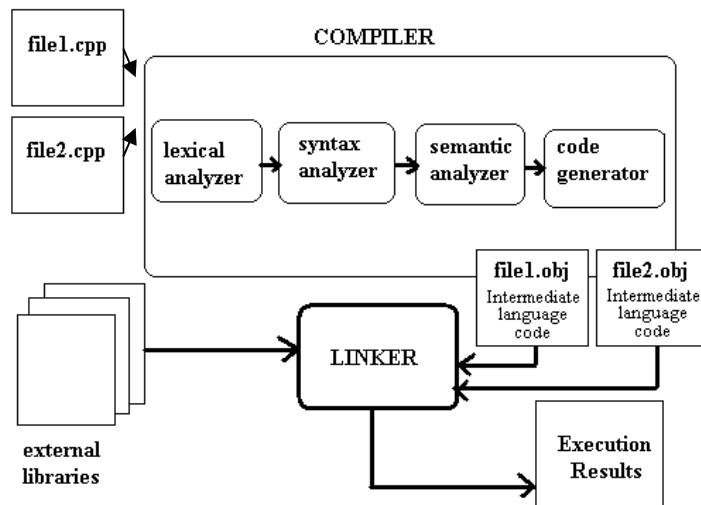
24. (a) CASE stands for 'Computer Aided Software Engineering'. CASE tools are automated software tools. CASE is the use of a computer-assisted method to organize and control the development of software, especially on large, complex projects involving many software components and people. Using CASE allows designers, code writers, testers, planners, and managers to share a common view of where a project stands at each stage of development. CASE helps ensure a disciplined, check-pointed process. A CASE tool may portray progress (or lack of it) graphically. It may also serve as a repository for or be linked to document and program libraries containing the project's business plans, design requirements, design specifications, detailed code specifications, the code units, test cases and results, and marketing and service plans.

Some of the benefits of CASE and similar approaches are that, by making the customer part of the process (through market analysis and focus groups, for example), a product is more likely to meet real-world requirements. Because the development process emphasises testing and redesign, the cost of servicing a product over its lifetime can be reduced considerably. An organised approach to development encourages code and design reuse, reducing costs and improving quality. Finally, quality products tend to improve an organisations image, providing a competitive advantage in the market.

- (b) CASE originated in the 1970s when computer companies were beginning to borrow ideas from the hardware manufacturing process and applied them to software development. Some CASE tools supported the concepts of structured programming and similar organised development methods. More recently, CASE tools have had to encompass or accommodate visual programming tools and object-oriented programming. A CASE tool may be part of a spectrum of processes designed to ensure quality in what is developed. Many companies have their processes audited and certified as being in conformance with the ISO 9000 standard. Some typical CASE tools are:

- Configuration management tools
- Data modelling tools

- Model transformation tools
  - Program transformation tools
  - Refactoring tools
  - Source code generation tools, and
  - Unified Modelling Language.
25. Programming workbench is made up of a set of tools to support the process of program development tools:
- (i) Language compiler: Translates host programs to object code. As part of a translation process, an abstract syntax tree and a symbol table is created.
  - (ii) Structured editor: Incorporates embedded programming language knowledge and edits the syntax representation of the program in the Abstract Syntax Tree (AST) rather than its source code text.
  - (iii) Linker: Links the object code program with components which have already been compiled.
  - (iv) Loader: Loads the executable program into the computer memory prior to execution.
  - (v) Cross referencer: Produces a cross-reference listing showing where all program names are declared and used.
  - (vi) Pretty printer: Scans the AST and prints the source program according to embedded formatting rules.
  - (vii) Static analyzer: Analyses the source code to discover anomalies such as un-initialised variables, unreachable code etc.



The flowchart demonstrates the process of compiling two source files (file1.cpp and file2.cpp) into object files (file1.obj and file2.obj) and further execution.

- (viii) Dynamic analyzer: Produces a source code listing annotated with the number of times each statement was executed when the program was run & generates information on program benches and loops and statistics of processor usage.
- (ix) Interaction debugger: Allows the user to control the execution sequence and view the program state as execution processes.