

PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

QUESTIONS

1. Define the following terms:
 - (i) System
 - (ii) Database
 - (iii) Data dictionary
 - (iv) Information
 - (v) Decision-making
 - (vi) Master file
 - (vii) Data Flow diagram (DFD)
 - (viii) Prototype
 - (ix) Piggybacking
 - (x) Integrated Test Facility
 - (xi) Dynamic Analyser
 - (xii) Snapshot Technique
 - (xiii) Test Data Generation
 - (xiv) Cross Compiler
 - (xv) Trojan horse
2. Define "Information". What are the characteristics of good or useful information?
3. (a) What are the major constraints in operating a MIS?
(b) Explain the four common cycles of a business activity.
4. Discuss the purpose of an Executive Information System.
5. Describe the various components of Client-Server Architecture.
6. (a) Explain and compare "top down" and "bottom up" approaches used for system development.
(b) Enumerate various important factors to be kept in mind while designing an output from an information system.
7. (a) Discuss briefly the guidelines on which the printed and visual display outputs are designed.
(b) Briefly discuss the four basic categories of system development tools? Discuss, in detail, some of the tools most widely used by the systems analyst.
8. (a) What is a system prototype and when is it used? Describe the system prototype process.
(b) Briefly describe the activities involved in conversion from manual to computerized system.
9. Draw a payroll flow chart explaining the processes involved.
10. (a) What is an ERP system? Bring out the major challenges involved in its implementation.
(b) Discuss the controlling costs pertaining to Enterprise Resource Planning.
11. (a) What do you understand by the term "Computer Frauds"? Discuss, in detail, the various controls which help to ensure the accuracy, integrity, and safety of system resources and also, increase the difficulty of committing fraud.
(b) Give an elaborate account on computer fraud and abuse techniques.
12. Detail the principles of Information Security.
13. Explain in brief the broad classes of input controls.
14. (a) Discuss various factors that yield manual audit method ineffective in Information System audit.
(b) Discuss the various issues that are of primary concerns for an auditor involved in information system audit.
15. Describe the major technique of concurrent Audit of Information Systems.
16. What is a programming CASE work-bench? Give some tools, which are part of a programming work-bench.

17. (a) Discuss Section 35 of chapter VII of the information Technology Act 2000 relating to Digital Signature Certificate.
(b) Discuss various sections relating to suspension and revocation of digital signature certificate.
18. (a) What do you understand by hash function with reference to electronic records ?
(b) Briefly describe Section 3 of Chapter II of Information Technology Act 2000 relating to Authentication of Electronic Records.
19. Write short notes on the following:
 - a. Risks involved in the End User Development approach.
 - b. Access controls in EDP set up.
 - c. Business Engineering.
 - d. Bench Marking problem for Vendor's Proposals.

SUGGESTED ANSWERS/HINTS

1. (i) System: It is a set of interrelated elements that operate collectively to accomplish some common purpose or goal. A business is an example of a system where economic resources such as people, money, material, machines etc. are transformed by various organizational processes into goods and services.
(ii) Database: It can be defined as a "super-file" which consolidates data records formerly stored in many data files. The data in database is organized in such a way that accesses to the data is improved and redundancy is reduced.
(iii) Data Dictionary: It is a computer file that contains descriptive information about the data items in the files of a business information system. Each computer record of a data dictionary contains information about a single data item used in a business information system.
(iv) Information: It 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. In other words, it is data that has been put into a meaningful and useful context.
(v) Decision-making: It is a managerial process and function of choosing a particular course of action out of several alternative courses for the purpose of achieving the organisations' goals. It involves committing the organization to specific courses of action and entails commitment of resources in specified ways.
(vi) Master file: It is a file containing relatively permanent information which is used as a source of reference and is generally updated periodically.
(vii) Data Flow Diagram: A data flow diagram (DFD) graphically describes the flow of data within an organization. It is used to document existing systems and to plan and design new ones.
(viii) Prototype: It is a working system with software that accepts input, performs calculations, and carries out other meaningful activities. It is designed to be evaluated by users and modified to suit their requirements.
(ix) Piggybacking: It refers to tapping into a communication line and latching on to a legitimate user before he can log on to the system.
(x) Integrated Test Facility (ITF): This is a concurrent audit technique that places a small set of fictitious records into master files.
(xi) Dynamic Analyser: It produces code listing annotated with the number of times each statement was executed, when the program was run.
(xii) Snapshot Technique: This is a concurrent audit technique that examines the way the transactions are processed by marking selected transactions with a special code.

- (xiii) Test Data Generator: It generates test data for the program to be tested. It may be accomplished by selecting data from a database or by using patterns to generate random data of the correct form.
 - (xiv) Cross Compiler: It is a compiler that runs on one platform and generates code for another machine. For example, a C++ compiler running in UNIX but generating code for use in Windows environment.
 - (xv) Trojan Horse: It is a program designed to capture username –ids and passwords from users without their knowledge.
2. 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. Information is the substance on which business decisions are based. The management plays the part of converting the information into action through the familiar 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 flows 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 of the above points, students are advised to refer to Study Paper, Chapter-1, Section 1.5.1.

3. (a) The following are the major constraints in operating a 'MIS':
- 1. 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, which 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. The criteria may be the need and importance of a function for which MIS can be installed first.
 - 3. Due to varied objectives of business concerns, the approach adopted by experts for designing and implementing MIS is a non-standardised one.
 - 4. Non- availability of cooperation from staff is a crucial problem. By organising lectures, showing films and explaining the utility of the system, they can be educated, some persons can be involved in the development and implementation of the system.
 - 5. There is high turnover of experts. It can be reduced by creating better working conditions.
 - 6. Difficulty in quantifying the benefits of MIS so that it is comparable with cost.
- (b) (i) Revenue cycle: Events related to the distribution of goods and services to other entities and the collection of related payments. It includes application systems involving customer order entry, billing, accounts receivable and sales reporting.
- (ii) Expenditure cycle: Events related to the acquisition of goods and services from other entities and the settlement of related obligations. It includes application systems

involving vendor selection and requisitioning, purchasing, accounts payable and payroll.

- (iii) Production cycle: Events related to the transformation of resources into goods and services. It includes application systems involving production control and reporting, product costing, inventory control and property accounting.
- (iv) Finance cycle: Events related to the acquisition and management of capital funds, including cash. It includes application systems concerned with cash management and control, debt management and the administration of employee benefit plans.

4. Purpose of EIS.

- (i) To support managerial learning about an organisation its work processes, and its interaction with the external environment so that managers can make better decisions.
- (ii) To allow timely access to information. Often by the time a useful report can be compiled by traditional method, the strategic issues facing the manager have changed and the report is never fully utilised.
- (iii) To direct management attention to specific areas of the organisation or specific business problems. Managers and subordinates can work together to determine the root causes of issues highlighted by EIS.
- (iv) Managers are particularly attentive to concrete information about their performance when it is available to their supervisors. This focus is very valuable if the information reported is actually important and represents a balanced view of the organisation's objectives.

5. Client-server model: 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 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-server 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 minimize 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.
6. (a) **TOP DOWN APPROACH**: The top down approach assumes and focuses on organizational goals, objectives and strategies. The logic here is that, above all, an information system needs to be responsive to and supportive of an organization's basic reasons for being. Hence the organization's goals should be the driving force behind development of all the computer systems.

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) Analyse the objectives and goals of the organization to determine where it is going and what management wants to accomplish. The analysis may be stated in terms of profits, growth, expansion of product line or services, diversification, increased market share and so on. It is also determined what resources are available in terms of capital, equipments and raw material.
- (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 analysed what decisions are made as well as 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. These factors provide many of the design specifications for the application systems.
- (e) Prepare specific information processing programs in detail and modules within these programmes. We may also identify files and database 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 systems, 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, file 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 integrated data enhances the shareability and evolvability of the database. It also ensures that uniform data are being used by all programs. Integrated data also provides added capability for inquiry processing and adhoc requests for reports.

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 analyzing 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 objectives 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 have a little role in the development of system under top down approach. Under bottom up approach, management refrains from guiding the development of system undertaken by supervisory level.
 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-systems. This system may not be integrated.
- (b) **DESIGNING SYSTEM OUTPUTS** : There are six important factors which should be considered by the system analyst while designing user outputs; these are: content, form, volume, timeliness, media and format. We will now discuss, in brief, various issues relating to above factors, which should be kept in mind.
- (i) *Content*: Content refers to the actual pieces of data included among the outputs provided to users. It is to be noted here that systems designers generally put too much content into managerial reports instead of too little. Too much content can cause managers to waste time in isolating the information that they need; it also diminishes the impact of truly important information. Hence, only the required information should be include in various outputs.
 - (ii) *Form*: Form refers to the way the content is presented to users. Content can be presented in various forms; quantitative, non-quantitative, text, graphics, video and audio. For example, information on distribution channels may be more understandable to the concerned manager if it is presented in the form of a map, with dots representing individual outlets for store. Various department managers often prefer both summary and detailed information to be presented in relative terms or in chart form such as a pie chart, line chart or bar chart rather than information in absolute terms. Sometimes, converting absolute values to relative values such as percentages often help managers to comprehended the data easily and make better decisions. Hence, the form of the output should be decided keeping in view the requirements for the concerned user.

- (iii) *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. Unusually heavy output volume normally causes concern about paper cost. In such a case, alternative methods of output display such as COM (Computer Output Microfiche) may be considered.
- (iv) *Timelines*: Timeliness refers to the frequency when users need outputs. Some outputs are required on a regular basis – perhaps daily, weekly, monthly, at the end of a quarter or annually. Other types of outputs are generated on request.
- (v) *Media*: Input-output medium 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. Many of these media are available in different forms. The system designer can select a medium, which is best suited to the user requirements.
- (vi) *Format*: The manner in which data are physically arranged is referred to as format.

The real issue in designing computer output is not how much can be provided, but how little is needed to make important information available. The major concern of the user in the system design effort is properly designed output, that is intelligent and decision impelling.

7. (a) 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. The 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, understandability and an esthetic appeal.

Visual display output : 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 lay out 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 center of the screen or in the upper left quadrant. However, it is mainly a matter of preference of the concerned system analysts.

(b) The four basic categories of system development tools are as follows:—

1. Components and flows of a system.
2. User interface
3. Data attributes and relationships.
4. Detailed system process.

The most widely used system development tools are given below:—

1. *System flow chart*: 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.
2. *Data flow diagrams*: These diagrams show graphically how data move within an organisation. In most instances, a data flow diagram shows logical descriptions of system elements.
3. *Layout forms and screens*: These consist of electronic displays or preprinted forms on which the size and placement of files, heading, data and information can be designed. These are used to design source documents, input/output and storage records, files and output displays and reports.
4. *System components matrix*: It views the information system as a matrix of components that highlights how the basic activities of input, processing, output, storage and control

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

5. *CASE tools*: CASE refers to the automation of anything that humans do to develop systems. It includes menu generators, source generators, reports generators, and code generator.
6. *Data Dictionary*: It is a catalogue or data base of meta-data, that is, 'data about data'. It describes the characteristics of the data elements and their inter-relationships. It may include description of data flows, data stores, and processes that affect them.

Students are required to describe these tools in detail as discussed in study paper, chapter 7, section 7.6.

8. (a) Hints: A prototype, a working system with software that accepts input, performs calculations, and carries out other meaningful activities, is designed to be evaluated by users and modified to suit their requirements. This method is likely to be most appropriate when no other system with the characteristics of the proposed one has yet been constructed by the team of developers; when the essential features of the proposed system are only partially known; when experience in using the system is likely to significantly add to the list of requirements the system must meet; when alternative versions of the system are likely to evolve, providing additional development and refinement of system features; and when users are able to participate in the development process.

Typically, the prototyping process begins with identification of the known requirements and features to be included in the system. Following the development of a working prototype, users interact with the model, noting what enhancements and changes are required. Using the expanded list of known systems requirements obtained through actual user experience with the system, developers revise the prototype. These steps are repeated as many times as necessary to achieve a system that satisfactorily meets the requirements of the users for whom it is developed.

Although actual development of the working prototype is the responsibility of systems analysts, user participation is essential. Both users and analysts meet to identify system requirements that will form the basis for construction of the prototype. As users gain experience in working with the actual prototype, they can point out desirable and undesirable features and thus provide valuable information on which to base revisions of the prototype. Finally, users and analysts collaborate in determining how to meet the system requirements identified as a result of the prototyping process, i.e., whether to redevelop the prototype, implement the prototype as the completed system, abandon the project, or begin another prototyping series.

- (b) Basically a changeover from manual to computerized system includes all those activities which must be completed successfully to convert from the previous system to the new information system. Fundamentally these activities can be classified into the broad categories as explained below:
 - (1) *Procedure conversion*: Operating procedure should be completely documented for the new system. This applies to both computer operations and functional area operations. 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 controls must be presented in clear, concise and understandable terms, both in written and oral form.
 - (2) *File Conversion*: Because large files of information must be converted from one medium to another, this phase should be started long before programming and testing are completed. The cost and related problem of file conversion are significant.

Computer files tend to be more accurate and consistent than manual files. The format of one computer file may be unacceptable for the other system. To be accurate, file conversion programs must be thoroughly tested and adequate controls must be generated. The existing computer files must be kept for some time as back-up, since they may be needed for reconstruction in case bug is discovered later on.

- (3) *System Conversion*: Now daily processing can be shifted from the existing system to a 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. If necessary, appropriate changes are made to the new system. The old system is dropped as soon as the data processing group is satisfied with the new system.
- (4) *Scheduling personnel and equipment* : Schedules should be set up by the system manager in conjunction with departmental managers of operational units. The time required to assign remote batch programs under normal operating conditions in real time is a problem, which is solved by designing a block of time each day for the operation of remote devices.

The equipment and the operating personnel must be scheduled for maximum utilization.

- (5) *Alternative plans in case of equipment failure*: Priorities must be given to those jobs critical to an organization such as billing, payroll and inventory. Documentation of alternative plans is the responsibility of the computer section and should be fully covered by the organisation's systems and procedures manual.
9. 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.

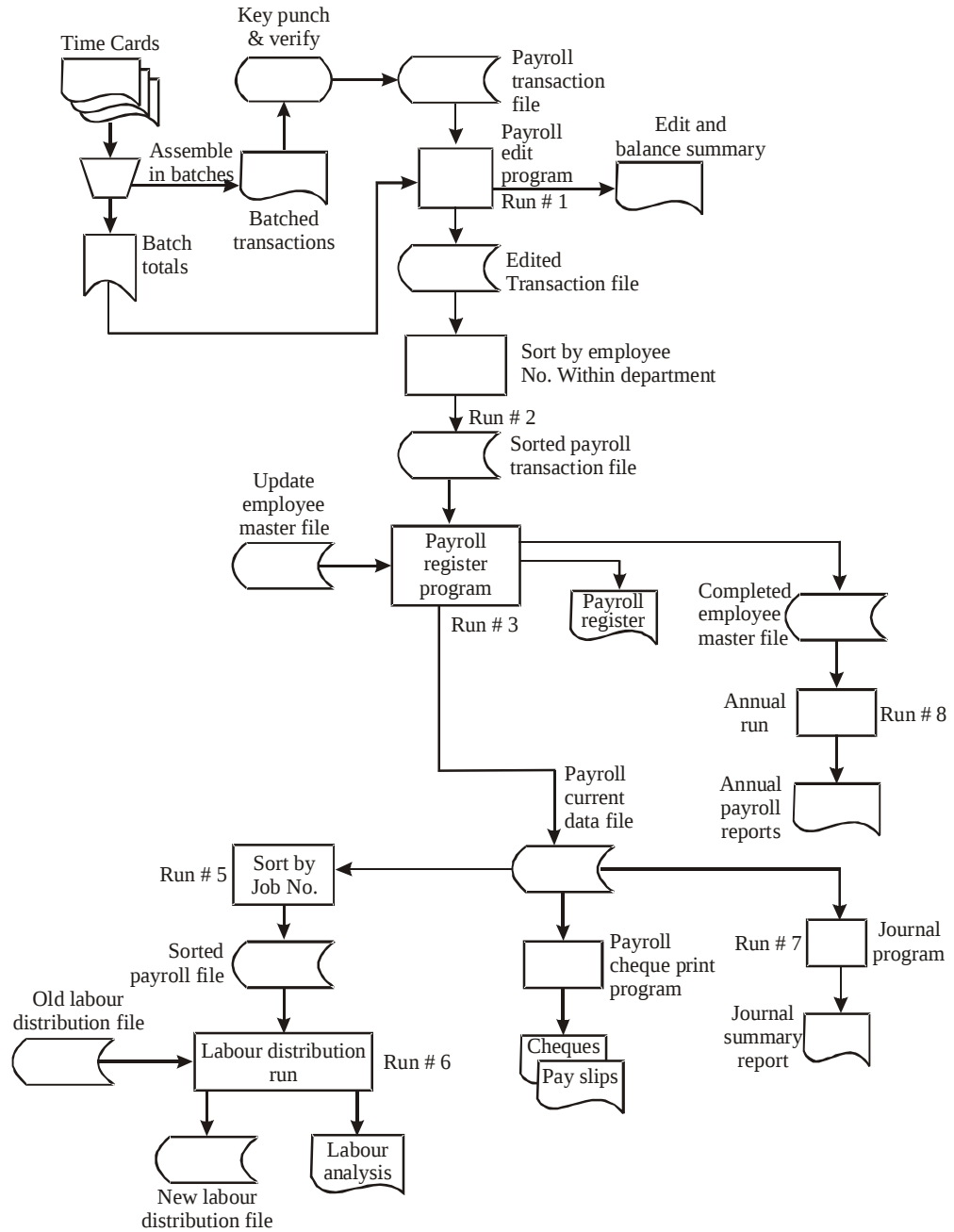
In run # 2, the payroll transaction file is sorted by the employee number within department number.

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 payslips 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 payslips.

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.

10. (a) ERP: 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 in the organization to make optimum use of resources such as men, material, money and machine. Simply stated, ERP promises one database, one application and one user interface for the entire enterprise. This helps in planning, monitoring and controlling the entire business.

The characteristics of an ERP system are: (1) Flexibility (2) Open system architecture (3) Comprehensive (4) On-line connectivity to other business entities (5) Collection of best business practices.

Some of the major features of ERP are: (1) Provides multi-platform, multi-facility, multi-currency, etc facilities (2) Supports strategic and business planning activities (3) Has end-to-end supply chain management (4) Provides intelligent business tools (5) Provides complete integration of systems (6) Better project management (7) Automatic introduction of latest technologies like EFT, EDI, Internet, etc.

The challenges involved in ERP implementation are:

- (i) Consultants, vendors and users have to work together to achieve the overall objectives of the organization. The consultants have to clearly understand the user needs and the prevailing business realities and design the business solutions keeping in mind all these factors.
- (ii) Proper customization of package to the organization has to be in tune with the users needs and business objectives.
- (iii) Roles and responsibilities of the employees have to be clearly identified, understood and configured in the system.
- (iv) Acceptance by employees for the new processes and procedures is critical for the success of the package.
- (v) Package to be implemented in totality to achieve the maximum benefit.
- (vi) Defining the implementation methodology to be followed – identifying needs, evaluation of the current situation, predicting the future situation, reengineering the business process, selection of correct package.
- (vii) Installation of Hardware, Software required for the package.
- (viii) Selection of right kind of consultants.

- (ix) Preparing the implementation guidelines – training users, effective leadership, adapting the new systems and making changes in the working environment etc.
 - (x) Post implementation monitoring of Key Performance indicators, Critical success factors etc.
- (b) The controlling costs related to ERP are as follows:
- (1) *Overhead Cost Control*: This focuses on monitoring and allocation of overheads. This cost cannot be directly assigned to the products manufactured or services given. This needs a transparent method of allocation.
 - (2) *Cost Center Accounting*: This analyses where overhead occurs within an organization. Costs are assigned to the sub areas of the organization where they are originated. Costs are allocated to products based on cost resources.
 - (3) *Overhead Orders*: This collects and analyses costs based on individual internal measures. It can monitor and check budgets assigned to each measure.
 - (4) *Activity Based Costing*: It is developed as the response to the need for monitoring and controlling cross departmental business processes in addition to functions and products.
 - (5) *Product Cost Control*: This determines the costs arising from the manufacture of a product or providing a service. A Control plan and standard values serve in evaluating warehouse stock and for comparing revenues received with costs. The values are crucial for determining the lowest price limit, for which a product is profitable.
 - (6) *Cost Object Controlling*: This helps in monitoring manufacturing orders. Calculations determine and analyse the variances between the actual manufacturing costs and plan costs resulting from product cost planning.
 - (7) *Profitability Analysis*: This examines sources of returns. As part of sales control, this is the last step in cost based settlement.
11. (a) Computer frauds can be 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 crime
 - Theft or destruction of computer hardware
 - Use or the conspiracy to use computer resources to commit an offence
 - Intend to illegally obtain information or tangible property through the use of computer.
- Controls that can be incorporate to ensure the accuracy, integrity and safety of system resources are:
- (i) Develop a strong system of internal controls
 - (ii) Segregate duties
 - (iii) Require vacations and rotate duties
 - (iv) Restrict access to computer equipments and data files
 - (v) Encrypt data and programs
 - (vi) Protect telephone lines

(vii) Protect the system from viruses.

For details to the above points, refer to study material, Chapter 15, Section 15.8.

- (b) Computer fraud and abuse techniques: Some of the techniques are briefly discussed below:

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	Unauthorised 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 message to try and get recipient to do something that would make it possible to defraud him.
Hacking	Unauthorised 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.
Internet terrorism	Using the Internet to disrupt electronic commerce and to destroy company and individual communications.
Logic time bomb	Program that lies idle until some specified circumstance or a particular time triggers it. Once triggered, the bomb sabotages the system by destroying programs, data or both.
Masquerading or impersonation	Perpetrator gains access to the system by pretending to be an authorized user. Enjoys same privileges as the legitimate user.
Password cracking	Intruder penetrates a system's defence, 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.
Superzapping	Unauthorised 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	Unauthorised 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.

12. The eight core principles of information Security are discussed below:

1. **Accountability:** Security of information requires timely apportionment of responsibility and accountability among data owners, process owners, technology providers and users. This accountability should be formalized and communicated. Issues relating to specification of ownership of data and information, identification of users and others who access the system, recording of activities and assignment of responsibility for maintenance of data and information etc. should be considered.
2. **Awareness:** In order to foster confidence in information data owners, process owners, technology providers and users must be able to gain knowledge of the existence and general extent of the risks facing the organisation and its system and the organization's security initiatives and requirements. Security measures are only effective if all involved are aware of their proper functioning and of the risks they address.
3. **Multidisciplinary:** Security covers technological, administrative, organizational, operational and legal issues. Technical standards should be developed with and enforced by codes of practice, audit, legislative, legal and regulatory requirements and awareness, education and training.
4. **Cost effectiveness:** Different levels and types of security may be required to address the risks to information. Security level and associated costs must be compatible with the value of the information. Following issues must be considered:
 - Value to and dependence of the organization on particular information assets.
 - Value of the data or information itself, based on a pre-defined level of confidentiality or sensitivity.
 - Threats to the information, including the severity and probability of such threats.
 - Safeguards that will minimize or eliminate the threats, including the costs of implementing the safeguards.
 - Costs and benefits of incremental increases to the level of security.

- Safeguards that will provide an optimum balance between the harm arising from a security breach and the costs associated with the safeguards.
 - Where available and appropriate, the benefit of adopting established minimum security safeguards as a cost-effective alternative to balancing costs and risks.
5. *Integration*: Measures, practices and procedures for security must be coordinated and integrated with each other and with other measures, practices, and procedures of the organisation, so as to create a coherent system of security. This requires that all levels of the information cycle are covered.
 6. *Reassessment*: The security of information system should be reassessed periodically, as information systems and the requirements for their security vary over time.
 7. *Timeliness*: Security procedures must provide for monitoring and timely response to real or attempted breaches in security in proportion with the risk. Following issues must be considered:
 - Instantaneous and irrevocable character of business transactions.
 - Volume of information generated from the increasingly interconnected and complex information systems.
 - Automated tools to support real-time and after-the –fact monitoring and
 - Expediency of escalating breaches to the appropriate decision making level.
 8. *Social factors*: Information and the security of information should be provided and used in such a manner that the rights and interests of others are respected. Level of security must be consistent with the use and flow of information.
13. 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.

Input controls are divided into the following broad classes:

- (i) Source document controls
- (ii) Data coding controls
- (iii) Batch controls
- (iv) Validation controls
- (v) Input error correction
- (vi) Generalised data input systems

These control classes are not mutually exclusive divisions. Some control techniques could fit logically into more than one class.

- (i) *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.

To control against this type of exposure, the organization must implement control procedures over source documents to account for each document as described below:

- Use prenumbered source documents
- Use source documents in sequence
- Periodically audit source documents

- (ii) *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.

- (iii) *Batch controls and hash totals:* They 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. Batch controls ensure that all records in a batch are processed, no records are processed more than once and an audit trail of transactions is created from input through processing to output stage of the system. Hash total uses non financial data to keep track of the records in a batch.
- (iv) *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.
- (v) *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.
- (vi) *Generalised Data Input Systems:* To achieve a high degree of control and standardization over input validation procedures, some organizations employ a generalized data input system (GDIS). This technique includes centralized procedures to manage the data input for all the organisation's transaction processing systems.

For further details, the students are advised to refer to study paper, Chapter 14, Section 14.1.

14. (a) The factors that yield manual audit method ineffective to Information System Audit are:

- (i) Electronic evidence
- (ii) Terminology
- (iii) Automated processes
- (iv) New risks and controls
- (v) Reliance on controls

Because the rate of these changes varies among systems in organizations, the methods and approaches of auditing automated IS differ among applications and organisations.

For details, students may refer to study paper, Chapter 17, Section 17.1.1.

- (b) 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 organisation'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.
- Authorisation 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.
- Databases 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 databases is updated concurrently.

This list affirms that the auditor is primarily concerned with adequate controls to safeguard the organization's assets.

15. 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) 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.
- (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.

16. 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 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) Petty 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.
- (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.

17. (a) Digital Signature Certification: Section 35 of chapter VII of the information Technology Act 2000 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 Certificate shall be granted unless the Certifying Authority is satisfied that-

- (i) the applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate;
- (ii) the applicant holds a private key, which is capable of creating a digital signature;
- (iii) 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.

(b) Suspension of digital signature certificate : 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.

18. (a) 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 :-
- (i) to derive or reconstruct the original electronic record from the hash result produced by the algorithm:
 - (ii) that two electronic records can produce the same hash result using the algorithm.
- (b) Authentication of Electronic Records Using Digital Signatures : Section 3 of Chapter II of Information Technology Act 2000 gives legal recognition to electronic records and digital signatures.

The 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 with since it was so fixed with the digital signature.

19. (a) End User Development Approach: Here the end user is responsible for system development activities. The end user is allowed to develop systems. The number and nature of systems development activities followed often differ from those found in formal approaches.

There are many advantages but a number of risks also are there. They are

- (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, which are unlikely in this approach.
 - (2) Inaccuracy of specification requirements as the end user may not have much experience.
 - (3) Due to the lack of adequate specifications, there would be a reduction in the quality assurance and stability of the system.
 - (4) An increase in unrelated and incompatible system. Hence, management would have difficulty in obtaining full corporate data.
 - (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.
- (b) Access Controls: In a shared database environment access control risks include corruption, theft, misuse and destruction of data. Several database control features are as follows:

- (1) User View: It is a subset of the total database that defines the user's data domain and provides access to the database. Although user views and restrict user access to a limited set of data, they do not define task privileges such as read, delete or write.
- (2) Database Authorization table: This contains rules that limit the actions a user can receive. This is similar to access list used in 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.
- (3) User Defined Procedures: This allows the user to create a personal security program to provide more positive user identification than a single password can e.g. a services of personal questions which only the legitimate user knows.
- (4) Data Encryption: Highly sensitive data like product formulas, password files etc. are protected by this. It uses an algorithm to scramble selected data and makes it unreadable to others. Also it protects data that are transmitted through networks.
- (5) Biometric Devices: This measures various personal characteristics such as finger prints, voice prints, signature etc. which are digitized and stored permanently in a database security file or on an identification card of the user.

- (c) Business Engineering: ERP is a result of a modern Enterprises concept of how the Information System is to be configured to the challenging environments of new business opportunities. Every company that intends to implement ERP has to engineer its processes in one form or the other. Business Engineering has come out of merging of two concepts, namely Information Technology and Business Process Reengineering.

It is the rethinking of Business Processes to improve speed, quality and output of materials or services. The emphasis is the concept of Process Oriented Business Solutions enhanced by the client-server computing in Information Technology. Here, the main point is the efficient redesigning of company's values added chains, which are a series of connected steps running through a business which when efficiently completed add value to enterprise and customers. Information technology helps to develop business models, which assist in redesigning of business processes.

Thus, Business Engineering is the method of development of business processes according to changing requirements.

- (d) Bench marking problem for Vendor's proposals: These are sample programs that represent at least a part of the buyer's primary computer work load. They include software considerations, Bench marking problems are oriented towards testing whether 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. If the job is truly represented by the selected bench marking problems, this approach can provide a realistic and tangible basis for comparing all vendors' proposals. Tests should enable buyer to effectively evaluate cross performance of various systems in terms of hardware performances.

But these problems take considerable time and effort to select problems representative of the job mix, which must be precisely defined. It also requires the existence of operational hardware, software and services of systems. However, they help the manager to extrapolate the performance of the vendor's proposal on the entire job mix.