

PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

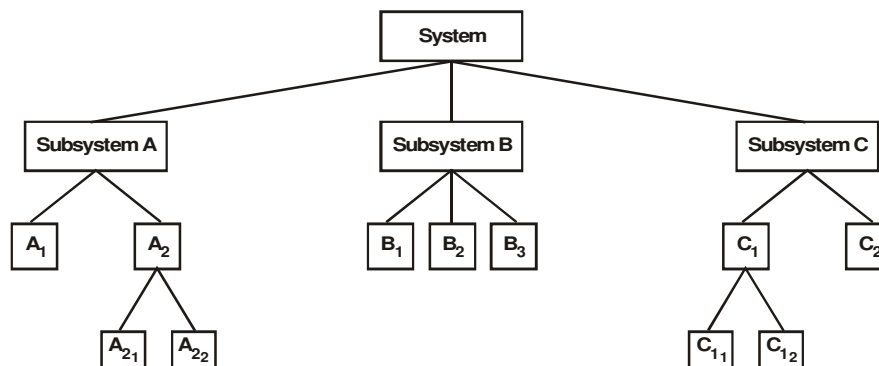
QUESTIONS

1. Explain the concept of decomposition with the help of an example.
2. Discuss, briefly, the various components of a Transaction Processing System (TPS)?
3. Describe, in brief, the impact of computers on management information system.
4. 'Finance and Accounting system is backbone of management information system.' Explain.
5. (a) Describe decision support systems (DSSs). What are their major components?
(b) 'Decision Support Systems are widely used as part of an organisation's Accounting Information System (AIS)'. Give examples to support this statement.
6. What are the control techniques that are essential for the security of the client/server environment?
7. (a) What is the systems development life cycle? What drawbacks are created with the systems development life cycle methodology?
(b) What do you understand by feasibility study? How is it conducted?
8. What do you understand by the term 'system design' ? Distinguish between logical design and physical design.
9. What basic features should be ascertained by the system analyst before purchasing packaged software? Enumerate them.
10. Describe briefly, various activities that should be completed for successful conversion of an existing system to the new information system.
11. Draw a flow chart for Cost Estimation System in on-line real time system. Discuss the system interfaces, inputs, output reports and files in this system.
12. What is Business Modelling? How can it be used for judging the suitability of ERP Package.
13. Explain briefly administrative and organizational controls in a computer-based system.
14. Describe, in brief, the three categories of processing controls.
15. (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 frauds.
(b) What are the primary risks to business organisations from computer frauds?
16. What is Digital Certificate and how it is issued? What are the rules regarding its suspension or revocation ?
17. (a) Discuss, briefly, the various factors that yield manual audit method ineffective in IS audit.
(b) What is an Audit Trail? In what ways does an audit trail safeguard both data and the organization in an online environment?
18. Why is information security important ? Does the degree of protection applied comprehends with the protection required ? If no, what is the reason for this gap ? Discuss about the type of threats faced by the information systems.
19. What do you mean by Integrated CASE tools? Describe the different levels of Integrated CASE tools, indicating the function performed by each.
20. Define the following terms:
 - (i) System
 - (ii) Database
 - (iii) Data dictionary
 - (ix) Piggybacking
 - (x) Integrated Test Facility
 - (xi) Dynamic Analyser

- | | |
|-------------------------------|-----------------------------|
| (iv) Information | (xii) Snapshot Technique |
| (v) Decision-making | (xiii) Test Data Generation |
| (vi) Master file | (xiv) Cross Compiler |
| (vii) Data Flow diagram (DFD) | (xv) Trojan Horse |
| (viii) Prototype | |

SUGGESTED ANSWERS/HINTS

1. A computer system is difficult to comprehend when considered as a whole. Therefore, it is better that the system is decomposed or factored into sub systems. The boundaries and interfaces are defined, so that sum of the sub systems constitute the entire system. This process of decomposition is continued with sub systems divided into smaller sub systems until the smallest sub systems are of manageable size. The sub systems resulting from this process generally form hierarchical structure as shown in the figure given below:



An example of decomposition is the factoring of an information processing system into sub systems. One approach to decomposition can be as follows:

- (a) Information system divided into sub system such as:-
- (i) Sales and order entry
 - (ii) Inventory
 - (iii) Production
 - (iv) Personnel and payroll
 - (v) Purchasing
 - (vi) Accounting and control
 - (vii) Planning
 - (viii) Environmental intelligence
- (b) Each sub system is divided further into sub systems. For example, the personnel and payroll sub system might be divided into the following smaller sub systems:-
- (i) Creation and update of personnel pay roll records
 - (ii) Personnel reports
 - (iii) Payroll data entry and validation
 - (iv) Hourly payroll processing
 - (v) Salaried payroll processing
 - (vi) Payroll reports for management

(vii) Payroll reports for Government

- (c) If the task is to design and programme a new system, the sub systems (major applications) defined above might be further sub divided into smaller sub systems or modules. For example, the hourly payroll processing sub system might be factored into modules for the calculation of deductions and net pay, payroll register and audit controls preparation, cheque printing and register and controls output.

Decomposition into sub systems is used to analyse an existing system and to design and implement a new system. In both the cases, the designer must decide how to factor i.e. where to draw the boundaries.

The general principle in decomposition, which assumes that system objectives dictate the process, is functional cohesion. Components are considered to be part of the same sub system if they perform or are related to the same function. The boundary then needs to be clearly specified, interfaces simplified and appropriate connections established among the subsystems.

2. The principal components of a transaction processing system are as enumerated below:

- (i). **Inputs:** It refers to the flow of data from the external sources within the boundaries of system. It includes the source data such as invoices of suppliers, purchase order, time cards of employees etc. It serves the following purposes :-

- (a) Capture data
- (b) Facilitate operations by communicating data and authorizing another operation in the process.
- (c) Standardize operations by indicating what data require recording and what actions need to be taken.
- (d) Provide a permanent file for future analysis, if the documents are retained.

Characteristics of Inputs:

- *External Sources:* It is the flow of data from the external sources within the boundaries of the system.
- *Unstructured:* This input is highly unstructured because it is coming from different sources on which the management has no direct control.
- *Input under computer system (Interfaces):* In case of computer based MIS, we must have highly structured format of data, therefore, it is the responsibility of system development team to develop an interface which can convert unstructured into structured inputs.

Depending upon the type of system, input can be:-

- **Batch Inputs:** Data is collected for a given time period e.g. purchase orders of one week are collected before taking suitable action.
- **Online Real Time Inputs:** Each transaction is immediately processed e.g. Railways, Reservation, Airline Reservation etc.

Devices of inputs to computer system: Different hardware devices e.g. MICR, OCR, OMR, Floppies etc. can be used as inputs to the computer system.

- (ii). **Processing:** It refers to transaction which needs to be carried out on a given set of inputs for converting it into the desired output.

In the case of computer based system, it refers to computer software i.e. collection of various programme to carry out the conversion of input data into required information.

Depending upon the type of system there are various types of programmes:

- (a) **Batch Processing:** There are five types of programmes in Batch processing:-

- Data Validation
- Data Sorting
- Merging Run
- Master File Updation Run
- Report Generation

(b) Online Real Time Processing: Each transaction is processed immediately when received and entered for updating the master file. There is no transaction file creation. Technique used for updating master file is "Updation By Overlay."

(iii). **Storage:** Ledgers and files provide storage of data in both manual and computerized systems. They provide summaries of a firm's financial accounting transactions.

Manual Storage Ledgers, cash books, and other records are prepared manually.

Computer Storage: A file is an organized collection of data.

There are several types of files as stated below:

Transaction file is a collection of transaction input data. Transaction files usually contain data that are of temporary rather than permanent interest.

A *master file* contains data that are of more continuing interest.

Reference file contains keys of records in other files. In order to retrieve a record from a file, the reference file is first searched to find out in which file a record can be located.

Table files are in the nature of catalogues of price lists.

Report file is created from records in other files in a meaningful and concise form. A sales performance report and a report on materials rejected are examples of report files.

Historical files contain statistical information of past periods. These files are used to analyse trends or make comparisons of one period with another and so on.

Back-up-files are copies of currently used master files kept in the computer library as a measure of security.

(iv). **Output:** It refers to the information which is produced within the boundaries of the system and transmitted to external agencies e.g. Invoices sent to the customers.

Since, it is produced within the system, the system designer has full control over its format and structure.

Depending upon the requirements output can be classified as:-

- *Hard Copy:* It is in the form of printed report which is normally preferred by human-beings for taking actions.
- *Electronic Copy (Soft Copy):* If output of one system becomes input for another system it is preferable to transmit it electronically e.g. –
 - By posting the data on a server in the case of computer network from where the other person can directly read with this program.
 - With the help of an electronic medium e.g. floppy disk. It is useful in case where the sender & receiver are not connected on a network.
 - In case of windows operating system output of one programme can be transferred as input to another programme with the help of cut & paste facility.

3. Management Information System or MIS is an old management tool which is being used by business managers as a means for better management and scientific decision making. It is a network of information that supports management decision-making. MIS provides for the identification of relevant information needs, the collection of relevant information, processing of the same to become usable by the business managers, and timely dissemination of processed

information to its users for properly managing the affairs of an enterprise by informed decisions. Schwartz defined MIS as a system of people, equipments, procedures, documents and communication that collects, validates, operates on transformers, stores, retrieves and present data for use in planning, budgeting, accounting, controlling and other management process. G.B. Davis defines MIS as “an integrated man/machine system for providing information to support the operations, management and decision making functions in an organisation”. The system utilises computer hardware and software, manual procedures, management and decision models and a data base.

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

- (i) **Speed of processing and retrieval of data increases:** Computers help in processing data with speed which in turn help in timely information. Efficient storage devices and databases help in fast and easy retrieval of information as per management requirements.
 - (ii) **Scope of use of information system has expanded:** Timely and accurate information increases the confidence of managers for decision making process and in-turn they rely more and more on information system for decision making processes.
 - (iii) **Scope of analysis widened:** Computers help in extracting and generating multiple type of information accurately and in no time for decision makers. This helps in widening analysis of problems.
 - (iv) **Complexity of system design and operation increased:** Use of computers require proper design and implementation of information systems, this in turn requires lot of hardware and software integration which is a complex task.
 - (v) **Integrates the working of different information sub-systems:** MIS allows a smooth and timely flow of information between various sub-systems of business organization, which helps in integration of business functions for achieving objectives of the organization.
 - (vi) **Increases the effectiveness of information systems:** The use of computer has increased the effectiveness of information systems also.
 - (vii) **More comprehensive information:** The use of computer for MIS enabled systems expert to provide more comprehensive information to executives on business matters.
4. **Finance and Accounting system:** Finance and accounting are separate functions but are sufficiently related. Accounting covers the classification of financial transactions and summarization into the standard financial statements (profit and loss account and balance sheet). Finance system ensures adequate organisational financing at a low cost so as to maximize returns to shareholders (owners). It comprises of major functions such as granting of credit to customers, collection process, cash management, financing capital and so on.
- Financial Decision Making:** Financial decision making deals with procurement of funds and their effective utilization in the business. Thus, there are two important aspects of financial decision-making. First relates to decisions regarding procurement of funds, and the second to decisions regarding effective utilization of funds in the business.
- Procurement of funds:** Procurement of funds is a complicated problem as there are number of sources from where the funds may be procured. Funds may be raised from various short-term sources such as banks, suppliers, credit etc. These sources have different characteristics in terms of risk, control and cost. The decision maker should make an analysis and decide for the options which involve minimum risk and cost.
- Utilisation of funds:** The next set of financial decisions relates to effective utilisation of funds. There are several long term and short term assets where funds are to be deployed. It is crucial for an organisation to employ funds properly and profitably. The funds are procured at a certain cost with level of risk. If they are not utilized in a manner so that they generate incremental income over their cost, there is no point in running the business. Thus, each decision should be properly analysed while investing in fixed assets.

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

- (i) *Estimation of requirement of funds:* A careful estimation of funds and the timing when they will be required is to be made. This can be done by forecasting all physical activities of the firm and translating them into monetary units.
- (ii) *Capital Structure Decision:* Decisions are to be taken to select an optimum mix of different sources of capital structure. There are various options available for procuring funds. Decision maker has to decide the ratio between debt 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:* Financial decision concerning profits and dividends are to be taken by decision maker. He has to ensure adequate surpluses in future for growth and distribution of dividends.
- (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 is concerned with investment of long term funds into current assets. Decisions are to be taken for effective financing of current assets required for day-to-day running of the organisation.
- (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.

So, financial decisions are very important for an organisation. A wrong financial decision may lead an organisation towards high losses. So, decision making in this field requires proper analysis and caution.

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 refer to study material, Chapter 5, Section 5.3.

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

- (i). **Cost Accounting System:** Many Industries like health care industry are well known for their cost complexity. Decision support systems can accumulate these product costs to calculate total costs per patient. Health care managers may combine cost

accounting decision support systems with other applications, such as productivity systems. Combining these applications allows managers to measure the effectiveness of specific operating processes. One health care organisation, for example, combines a variety of decision support system applications in productivity, cost accounting, case mix, and nursing staff scheduling to improve its management decision making.

- (ii). **Capital Budgeting System:** Companies require new tools to evaluate high technology, investment decisions. Decision makers need to supplement analytical techniques, such as net present value and internal rate of return, with decision support tools that consider some benefits of new technology not captured in strict financial analysis. One decision support system designed to support decisions about investments in automated manufacturing technology is AutoMan, which allows decision makers to consider financial, non-financial, quantitative, and qualitative factors in their decision-making processes. Using this decision support system, accountants, managers, and engineers identify and prioritise these factors. They can then evaluate up to seven investment alternatives at once.
 - (iii). **Budget variance analysis System:** DSS is used to analyse the utilization of budgets and corresponding performances etc.
 - (iv). **Product Costing:** This is used to analyse or decide the cost of product as per various input and output conditions like cost of raw material, margin required, volume etc.
 - (v). **General Application:** Some planning languages used in DSS are general purpose and therefore have the ability to analyze many different types of problems. These can be used for:
 - (a) Ratio Analysis
 - (b) Balance Sheet Analysis
 - (c) Cash Flow Analysis
 - (d) Receivable Analysis
 - (vi). **Portfolio Management:** Equity Analyst uses DSS to analyse the company equities for various parameters, income, P/E Ratio, Economic conditions etc. and output of DSS supports analyst to forecast equity price etc.
6. To increase the security of a client/server environment, an Information System (IS) auditor should ensure that the following control techniques are in place:-
- **Access to data** and application is secured by disabling the floppy disk drive.
 - **Diskless workstation** prevents unauthorised access.
 - Unauthorized users may be prevented from overriding login scripts and access by securing **automatic boot or startup** batch files.
 - **Network monitoring** can be done to know about the client so that it will be helpful for later investigation, if it is monitored properly. Various network monitoring devices are used for this purpose. Since this is a detective control technique, the network administrator must continuously monitor the activities and maintain the devices, otherwise these tools become useless.
 - **Data encryption** techniques are used to protect data from unauthorized access.
 - **Authentication systems** can be provided to clients, so that they can enter into system, only by entering login name and password.
 - **Smart cards** can be used. It uses intelligent hand held devices and encryption techniques to decipher random codes provided by client-server based operating systems. A smart card displays a temporary password based on an algorithm and must be re-entered by the user during the login session for access onto the client-server system.

- **Application controls** may be used and users will be limited to access only those functions in the system that are required to be performed for their duties.

7. (a) The process of system development starts when management realizes that a particular business needs improvement. The systems development life cycle (SDLC) can be thought of as a set of activities that analysts, designers and users carry out to develop and implement an information system. The systems development life cycle method consists of the following activities:

- Preliminary investigation
- Requirements analysis or system analysis
- Design of system
- Development of software
- Systems testing
- Implementation and maintenance

The SDLC should be viewed as a continuous interactive process that recycles through each stage for many applications. Thus, even when a system is fully specified, designed, purchased and running, it is continually being enhanced or maintained.

Drawbacks of SDLC methodology: Some of the drawbacks created with the SDLC methodology are:

- SDLC methodologies do not work well for small projects that require rapid development or heavy user involvement with many changes.
- The formality of SDLC increases the cost of development and lengthens the development time.
- Rigidity of SDLC tends to make it difficult to develop many modern applications.
- It becomes very difficult to estimate costs and as a result, projects overrun the budgets.

For details, refer to Chapter 7, Section 7.1 and 7.2 of the study material.

(b) Feasibility study refers to a process of evaluating alternative systems through cost/benefit analysis so that the most feasible and desirable system can be selected for development. The feasibility study of a system is undertaken from three angles: technical, economic and operational feasibility. The proposed system is evaluated from a technical view point first and if technically feasible, its impact on the organization and staff is assessed. If a compatible technical and social system can be devised, it is then tested for economic feasibility.

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

- Does the necessary technology exist to do what is suggested (and can it be acquired) ?
- Do the proposed equipments have the technical capacity to hold the data required to use the new system ?
- Will the proposed system provide adequate responses to inquiries, regardless of the number or location of user ?
- Can the system be expanded if developed ?
- Are there technical guarantees of accuracy, reliability, ease of access, and data security ?

2. **Economic feasibility:** It includes an evaluation of all the incremental costs and

benefits expected if the proposed system is implemented. This is the most difficult aspect of the study. The financial and economic questions raised by analysts during the preliminary investigation are for the purpose of estimating the following:

- (i) The cost of conducting a full system investigation.
- (ii) The cost of hardware and software for the class of applications being considered.
- (iii) The benefits in the form of reduced costs or fewer costly errors.
- (iv) The cost if nothing changes (i.e. the proposed system is not developed)

The procedure employed is the traditional cost-benefit study.

3. **Operational Feasibility:** It is concerned with operational parameters in terms of employees, customers and suppliers etc. about the use of computer facilities. Some of the questions which help in testing the operational feasibility of a project are:

- Is there sufficient support from the users, management ?
- Are the current business methods acceptable to users ?
- Are the users involved in the planning and development of the project ?
- Will there be loss of control, slower processing etc. ?

There are other two feasibilities also which may be determining factors from time and legal aspects. These are:

4. **Schedule Feasibility:** This feasibility relates to time estimates - how much time a particular option for a project will take. Management may take decision on this basis whether proposed time is acceptable for system development or not.
5. **Legal Feasibility:** This is mainly concerned with whether there will be any conflict between newly proposed system and organization's legal obligations.

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

- (i) Reviewing the system's informational and functional requirements;
- (ii) Developing a model of the new system, including logical and physical specifications of outputs, inputs, processing, storage, procedures and personnel;
- (iii) Reporting results to management.

Objective: The systems analyst should try to design such a system which must conform to the purpose, scale and general concepts of the system that management approved during the requirements analysis phase.

System design involves first logical design and then physical construction of a system:

When analysts formulate a logical design, they write the detailed specification for the new system. They describe its features, the outputs, input files, database and procedures, all in a manner that meets system's requirements. The statement of these features is termed as the design specifications of the system.

Logical Design: The logical design of an information system is like an engineering blueprint; it shows major features of the system and how they are related to one another. The reports and outputs of the system are like the engineer's design components. Data and procedures are linked together to produce a working system.

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

Developing a model for a new system: When designing a system, the systems analysts and systems development team should design the following and their relationship with each other.

(i) Outputs, (ii) Inputs, (iii) Processing, (iv) Storage, (v) Procedures, and (vi) Personnel.

9. The following features of a packaged 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?
- (xiv) Is comprehensive documentation available ?
- (xv) Who will maintain the package ?
- (xvi) What are the package constraints ?
- (xvii) Where is the package currently utilised ?
- (xviii) What is the primary language?
- (xix) What input/output techniques are utilised ?
- (xx) What are the required input/output formats ?
- (xxi) How must input be organised ?
- (xxii) What kind of user training is provided?

10. System conversion involves changing from the old system to the new information system with the following activities:

- **Procedures Conversion:** Operating procedures must be clearly defined and documented for the new system. These procedures apply to both computer-operation and functional areas. Changes may be required for –
 - (i) *Input:* The manual documents, which are handwritten, may have to be replaced with new documents using magnetic ink in the case of MICR/Bar codes.
 - (ii) *Process Change:* The procedure for carrying out the processing of input data may have to undergo a change e.g., manual tellers in the bank may need to be replaced with the help of ATM's to facilitate online transactions by the user.

(iii) **Output Conversion:** The format and the procedures for the output reports may undergo change e.g. manually entered passbook in a bank replaced with a monthly computer printed statement of account.

- **File conversion:** The old data files should be converted to new system and these conversions should be done before the system is implemented. Data file conversion is one of the most important tasks and it should be done with utmost care. An old file should also be kept for some time if any bug is detected later on in new converted data files.

Based upon the new system, the data files have to be organized by selecting a suitable file organisation technique e.g. self-addressing, indexed, non-sequential etc.

- **System (Processing) Conversion:** After data files are converted from old system to new system and system components are properly in place, users in organization should start working on new system. If required, for some time old system may be continued for verification purpose. But once every thing is okay, users can start using new system completely.

These are important in the on-line real time systems where data entry can be done directly by external agencies e.g. in the case of e-commerce applications, the customers can place orders and make payments electronically through the Internet. Therefore, necessary changes have to be incorporated within the system to allow such transactions.

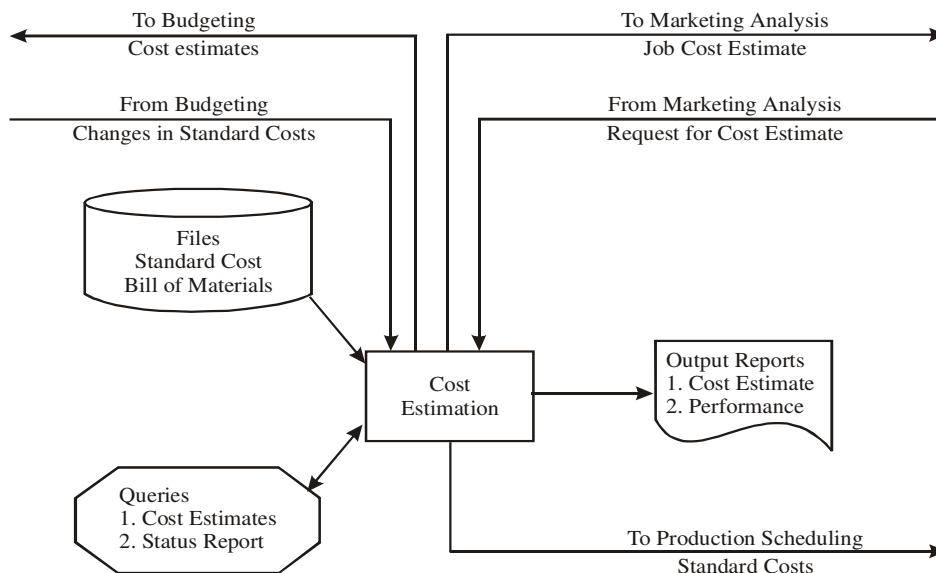
- **Scheduling of personnel and equipment:** This should be done for productive use of personnel working on system. Schedule should be set up for both equipments and personnel, for data processing activities so that required outputs are available on time.
- **Preparation of alternative plan in case of equipment failure:** Once a new system is implemented, an alternative plan for data processing should always be there in case of equipment failure. Particularly with use of online system, there should be enough back-up system and for taking up the process in case of main equipment failures. Disaster recovery team and plan should be there and should be implemented.

11. **Cost Estimation System:** The cost estimation system provides manufacturing cost estimates based on enquiries received from potential customers.

System Interfaces:

Marketing System: For request for cost estimates and Job cost estimates

Budgeting System: System reports for any changes in standard, material, machine and overheads cost.



Summary reports of all cost estimates are transferred to budgeting system and used to prepare annual budget for the firms.

Production Scheduling System: Once the order is received, standard cost for the job are transferred to the production scheduling system.

Files and Inputs: There are basically two files: (1) Standard Cost (2) Bill of Materials

In standard cost files, standard costs are maintained for each labour, material and machine as well as manufacturing operations. These costs are the basis for preparing manufacturing cost estimates.

The standard costs are updated on the basis of information provided by the budgeting system.

Cost estimation system also maintains information about bill of materials. This file contains list of all materials required to produce each product. This file also includes approved vendors for each materials.

Reports: (1) Cost Estimates (2) Cost Estimation Performance Reports.

12. *Business Modelling:* The approach to ERP development is first developing a business model comprising the business processes or activities that are essence of the business. This is not a mathematical model, but the portrayal of a business as one large system showing the interconnection and sequence of the business subsystems or processes that drive it. Based on business strategy and objectives, a business model consisting of business processes is developed. The approach of ERP implementation is carried out using MIS planning. The planning to arrive at the process in ERP implementation is from top down whereas the MIS implementation is done from bottom up.

These processes are managed and controlled by various individuals in various organizations. ERP is developed to provide the required information to the organization to manage the process that are part of the business model. The database is source of information and drives the ERP.

Business can be modelled as a system comprising of the processes of managing their facilities and material as their resources. Information is treated as a vital resource managing other resources. Business Model consists of two main elements:-

- (i) Blue print describing various business processes and their interactions.
- (ii) Underlying data Model.

Features of one Business Model (SAP)

- (i) Represents Business Processes.
- (ii) Comprehensive Functionality.
- (iii) Designed for all types of businesses.
- (iv) Multi-national.
- (v) Business engineering.
- (vi) Client-Server architecture.
- (vii) Open System.

Business Modeling in Practice: Most of the ERP packages available today enable flow charting business processes using standard flow chart symbols. By connecting symbols used for users, events, tasks/functions, and other organizational information, complex business information can be analysed. For example, SAP which is a popular ERP package uses event driven process chain (EPC) methodology to model Business Processes. All ERP packages provide standard template for each of the processes so that actual processes can be compared and deviation analysed.

With the help of the business model, it is possible to check as to how well the model fits into the application so that the degree of suitability of the ERP packages can be assessed. Business Modelling is the basis by which one can select and implement a suitable ERP package.

13. Administrative and organizational controls are those, which are designed to ensure that an acceptable standard of discipline and efficiency is maintained over the day-to-day running of the computer department. They are usually of more importance in computer based systems than in other accounting systems. An efficient administrative and organizational control system will involve the following steps:
 - (i) **Segregation of duties:** There should be a clear division of responsibility, not only between computer and user departments, but also within the computer department itself.
 - (ii) **Control over personnel managing the computer department:** Suitable controls should be developed for the operators and data preparation staff. This can be achieved by proper supervision and review of computer log, development of well prepared operator's instruction manuals, designing suitable software checks (say, against incorrect file loading) and restricting the use of computer to authorised personnel only.
 - (iii) **Physical protection and security against fire hazards:** There should be adequate arrangements for physical security such as:
 - environment protection like air conditioning, use of temperature and humidity records and dust detectors.
 - restriction of computer access to authorised personnel only.
 - preserving data files and programs in fire proof cabins and almirahs retaining duplicate copies of all important master files and programs at some other location.
 - ensuring that machines which may damage the contents of magnetic storage are not used near magnetic files.
 - (iv) **File controls:** These are important since even in a small computer installation, the number of files may run into scores. Control procedures should ensure that only the correct file can be used and that no file can be used for an unauthorised purpose. File control procedures include file storage procedures, file identification procedures, and file reconstruction procedures.
 - (v) **Stand-by arrangements and insurances:** Stand-by procedures include the use of an alternative computer installation or introduction of manual system in the event of a prolonged break down of the equipment. It should also be ensured that live files can be reconstructed if their contents are inadvertently destroyed. Also, proper insurance cover should be arranged in respect of hardware and software. Employee fidelity insurance should be arranged to minimise losses through fraudulent activities of employees.
14. After passing through the data input stage, transactions enter the processing stage of the system. Processing controls are divided into three categories: run-to-run controls, operator intervention controls, and audit trail controls.
 1. **Run-to-Run Controls:** Run-to-run controls use batch figures to monitor the batch as it moves from one programmed procedure (run) to another. These controls ensure that each run in the system processes the batch correctly and completely. Batch control figures may be contained in either a separate control record created at the data input stage or an internal label. Specific uses of run-to-run control figures are described below.

Recalculate Control Totals: After each major operation in the process and after each run, amount fields, hash totals, and record counts are accumulated and compared to the corresponding values stored in the control record. If a record in the batch is lost, goes unprocessed, or is processed more than once, this will be revealed by the discrepancies between these figures.

Transaction Codes: The transaction code of each record in the batch is compared to the transaction code contained in the control record. This ensures that only the correct type of transaction is being processed.

Sequence Checks: As the batch moves through the process, it must be re-sorted in the order of the master file used in each run. The sequence check control compares the sequence of each record in the batch with the previous record to ensure that proper sorting took place.

2. **Operator Intervention Controls:** Systems sometimes require operator intervention to initiate certain actions, such as entering control totals for a batch of records, providing parameter values for logical operations, and activating a program from a different point when re-entering semi-processed error records. Operator intervention increases the potential for human error. Systems that limit operator intervention through operator intervention controls are thus less prone to processing errors. Although it may be impossible to eliminate operator involvement completely, parameter values and program start points should, to the extent possible, be derived logically or provided to the system through look-up tables.
3. **Audit Trail Controls:** The preservation of an audit trail is an important objective of process control. In an accounting system, every transaction must be traceable through each stage of processing from its economic source to its presentation in financial statements. In a Computer based Information System (CBIS) environment, the audit trail can become fragmented and difficult to follow. It thus becomes critical that each major operation applied to a transaction be thoroughly documented. The following are examples of techniques used to preserve audit trails in a CBIS:

- (a) *Transaction Logs:* Every transaction successfully processed by the system should be recorded on a transaction log, which serves as a journal.

There are two reasons for creating a transaction log. First, the transaction log is a permanent record of transactions. The validated transaction file produced at the data input phase is usually a temporary file. Once processed, the records on this file are erased (scratched) to make room for the next batch of transactions. Second, not all of the records in the validated transaction file may be successfully processed. Some of these records may fail tests in the subsequent processing stages. A transaction log should contain only successful transactions – those that have changed account balances. Unsuccessful transactions should be placed in an error file. The transaction log and error files combined should account for all the transactions in the batch. The validated transactions may then be scratched with no loss of data.

- (b) *Transaction Listings:* The system should produce a (hard-copy) transaction listing of all successful transactions. These listing should go to the appropriate users to facilitate reconciliation with input.
- (c) *Log of Automatic Transactions:* Some transactions are triggered internally by the system. An example of this is when inventory drops below a preset reorder point, and the system automatically processes a purchase order. To maintain an audit trail of these activities, all internally generated transactions must be placed in a transaction log.
- (d) *Listing of Automatic Transactions:* To maintain control over automatic transactions processed by the system, the responsible end user should receive a detailed listing of all internally related transactions.
- (e) *Unique Transaction Identifiers:* Each transaction processed by the system must be uniquely identified with a transaction number. This is the only practical means of tracing particular transaction through a database of thousands or even millions of records. In systems that use physical source documents, the unique number printed on the document can be transcribed during data input and used for this purpose. In real-time systems, which do not use source documents, each transaction should be

assigned a unique number by the system.

- (f) *Error Listing:* A listing of all error records should go to the appropriate user to support error correction and resubmission.

15. (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 time
- 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 incorporated 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 of employees 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) Risks to business from computer fraud may be in the nature of internal threats, external threats, intrusions by outsiders etc., which are described as follows:-

- (i) **Internal Threats:** It is a greater risk to business as compared to external threats. One way to categorise computer frauds is to use the data processing model: input processor, computer instructions, stored data and output.

(a) *Input:* Input alteration is the simplest, most common way requiring a little knowledge of computer to commit a fraud. But the perpetrator should understand how the system operates.

- *Collusive fraud:* The perpetrator opens a bank account and then replaces all the deposit slips with the similar looking slips with his account number encoded on them. He may withdraw the money and disappear.
- *Disbursement frauds:* In this perpetrator either causes a company to pay too much or to pay for goods that were never ordered.
- *Payroll frauds:* Insertion of dummy employees or retention of records of a terminated employee. Under both the cases, the perpetrator proceeds to intercept and cash the illegal cheques.
- Cash receipt fraud includes non-entering of the cash receipt or entering with a lesser amount.

(b) *Processor :* Computer fraud can be committed through unauthorized system use, including the theft of computer time and services. Most people call it employee goofing.

(c) *Computer instructions:* Computer fraud can be accomplished by tampering with the

software that processes the data. This involves modifying the software, making illegal copies or using it in an unauthorized manner. It might also involve developing a software program or module to carry out an unauthorized activity. This approach to computer fraud used to be the least common because it requires specialized knowledge about programming.

- (d) *Data*: Computer fraud can be perpetrated by altering, damaging, stealing, copying, using or searching them without authorisation. There have been numerous instances of data files being scrambled, altered, or destroyed by disgruntled employees.
 - (e) *Output*: Computer fraud can be carried out by stealing or misusing system output. System output is usually displayed on monitors or printed on paper.
 - (f) *Malicious alterations of e-mail*: This can happen when an employee has a grudge against another member of staff or management. The effects can be troublesome, if not damaging.
- (ii) **External threats:** (Hacking) Main threat from hacking are:-
- (a) Removal of Information,
 - (b) Destruction of system integrity,
 - (c) Interference with web pages,
 - (d) Transmission of virus by e-mail,
 - (e) Interception of e-mail,
 - (f) Interception of electronic payments.

16. Digital Certificate is used to ensure the receiver that the sender's public key is valid. For this purpose sender has to obtain a Digital Certificate from a Certification Authority. It is a proof that public key with receiver belongs to the person who has claimed for this. Certification Authority certifies public key by digitally signing the sender public key with authority private key and authority puts his sign on Digital Certificate. And any user who wants to use some one's public key can verify its validity by applying the certification authority public key to the certificate. In this way, user would get actual public key of the sender and can tally this public key with the public key supplied by sender.

Procedure for issuance of a Digital Signature Certificate: Section 35 lays down that an application for such certificate shall be made in the prescribed form and shall be accompanied by a fee not exceeding Rs. 25,000. The fee shall be prescribed by the Central Government, and different fees may be prescribed for different classes of applicants.

The section also provides that no Digital Signature Certificate shall be granted unless the Certifying Authority is satisfied that –

- (a) the applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate;
- (b) the applicant holds a private key, which is capable of creating a digital signature;
- (c) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant.

No application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

While issuing a Digital Signature Certificate, the Certifying Authority should certify that it has complied with the provisions of the Act, the rules and regulations made there under and also with other conditions mentioned in the Digital Signature Certificate.

Suspension / Revocation 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 Certificates* under certain circumstances. Such revocation shall not be done unless the subscriber has been given an opportunity of being heard in the matter. Upon revocation or suspension, the Certifying Authority shall publish the *notice of suspension or revocation* of a Digital Signature Certificate.

17. (a) The audit methods that are effective for manual audits prove ineffective in many IS audits because of these factors:-

- (i) *Electronic Evidence*: In a manual system each data is available in the form of a hard copy and it can be verified by the auditor for authorization and checking but in computer system, essential evidence is not physically retrievable by most auditors, and it is not readable in its original electronic form.
- (ii) *Terminology*: The tools and techniques used in automated applications are described in terms that are difficult for the non-EDP auditor to understand.
- (iii) *Automated Process*: The methods of processing are automated rather than manual, making it difficult for the non-EDP auditor to comprehend processing concepts and the logic of these concepts.

In the case of integrated system, a large number of programs are combined into single program making it very large and complex. The step by step logic can be understood by the auditor if he has some programming knowledge.

- (iv) *New risks and controls*: Threats to computer systems (e.g. virus, hardware failure, software errors and frauds) and the countermeasures to those threats (i.e. controls) are new to non-EDP auditors, and the magnitude of the risks and the effectiveness of the controls are not understood.

The auditor should have the knowledge of these risks and controls. There are two types of controls –

- General Controls;
- Application Controls.

Auditor should take care of these to make his audit effective.

- (v) *Reliance on controls*: In manual systems, the auditor can place some reliance on hard-copy evidence, regardless of the adequacy of the controls, whereas, in automated systems, the electronic evidence is only as valid as the adequacy of controls.

Due to these factors manual system's audit techniques are ineffective in computerized systems. Since the rate of these changes is not same for all organizations so the methods and approaches of audit differ in different organisations. Auditor can make his audit effective by having the knowledge of computer systems, its risk and controls.

- (b) Audit Trails are logs that can be designed to record activities at the system, application, and user level. When properly implemented, audit trails provide an important detective control to help accomplish security policy objectives.

The audit trail helps safeguard both data and the organization in an online environment in the following ways:

- (i) Detecting unauthorized access to the system;
- (ii) Facilitating the reconstruction of events; and

- (iii) Promoting personal accountability.

For details, refer to Chapter 13, Section 13.2.5 of the study material.

18. Importance of Information Security :-

- (i) In a global information society, information travels through cyberspace on a routine basis.
- (ii) Organisations depend on timely, accurate, complete, valid, consistent, relevant and reliable information.
- (iii) The information is transmitted with the help of communication devices at different locations with the help of LAN, WAN, and Internet.
- (iv) Most of the organizations have adopted client server architecture where complete information is normally available on a server accessible by the clients from remote locations.

Therefore, management is responsible for maintaining confidentiality and security of such information. There are not only benefits from the use of information systems, there are many risks relating to the information systems. These risks have led a gap between the need to protect systems and the degree of protection applied. This gap is caused by:-

- (i) Widespread use of technology;
- (ii) Interconnectivity of systems;
- (iii) Elimination of distance, time, and space as constraints;
- (iv) Unevenness of technological changes;
- (v) Devolution of management and control;
- (vi) Attractiveness of conducting unconventional electronic attacks over more conventional physical attacks against organizations; and
- (vii) External factors such as legislative, legal, and regulatory requirements or technological developments.

Types of threats faced by an information system are:

- (i) *Technological Threats* e.g. bugs in the program which may spoil the information and system, e.g., disk crashes.
- (ii) *Natural Threats* e.g. floods and fire etc.
- (iii) *Unauthorised Access* by external sources e.g. hacking on the network and introduction of computer virus.
- (iv) *Unintentional Threats* e.g. lack of training, errors and omissions.
- (v) *Business dependencies* such as reliance on their party communications carriers, outsourced operations.

19. Integrated CASE tools : Specialised CASE tools can be combined together to provide a wider support to software process activities. An effective integration for framework makes evolution possible as new systems are added without disturbing the existing systems. In system engineering environment, there are five different levels of integration of CASE tools which are possible.

- (i) *Platform integration*: Tools run on the same hardware/ operating system platform.
- (ii) *Data integration*: Tools operate using a shared data model.
- (iii) *Presentation integration*: Tools offer a common user interface.
- (iv) *Control integration*: Tools may activate and control the operation of other tools.
- (v) *Process integration*: Guided by a process model.

For details, refer to Chapter 19, Section 19.2.1 of the study material.

20. (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 transaction 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.