

PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS
QUESTIONS

Basic Concepts of Systems

1. (a) Define the term 'Stress'. Also explain the types of stress.
(b) Discuss the experts systems in brief.

Transaction Processing System

2. Define the following terms:
 - (i) Transaction File
 - (ii) Master File
 - (iii) Reference File

Basic Concepts of MIS

3. (a) Discuss the activities required to perform by a manager in an organization.
(b) Describe the important characteristics of an effective MIS.
4. (a) How will you evaluate an MIS? Explain in brief.
(b) Explain the limitations of MIS.

System Approach and Decision Making

5. (a) Give the steps in the process of decision making in brief.
(b) Explain various financial decisions made with the help of Financial Information System.
6. (a) Discuss the information required for the purpose of planning in the case of a marketing system.
(b) Explain the information sub systems to increase the operational efficiency of personnel management.

Decision Support and Executive Information Systems

7. (a) Discuss the purposes of an Executive Information System.
(b) Give some practical set of principles to guide the design of measures and indicators to be included in an Executive Information System.

Enabling Technologies

8. (a) Explain the ten key characteristics of Client/Server Technology.
(b) Discuss the client / server risks in brief.

System Development Process

9. (a) Discuss the disadvantages of prototyping approach.
(b) Explain the risks involved in the end user development approach.

FINAL (OLD) EXAMINATION: NOVEMBER, 2010

10. (a) Discuss the accountants' involvement in development work.
(b) Describe the objectives which should be accomplished by the analyst working on the preliminary investigation.
11. (a) Explain the terms 'Schedule Feasibility', and 'Legal Feasibility'.
(b) Discuss the contents of Operational Costs of a computer based information system.

Systems Design

12. (a) "Designing a layout begins with verifying the characteristics of the display screen." Discuss it?
(b) Discuss some desired characteristics of a good coding scheme.

System's Acquisition Software Development and testing

13. (a) Discuss the important factors to be considered towards rigorous evaluation of vendors' proposals.
(b) Give some examples of Support Service Checklists.

Systems Implementation and Maintenance

14. (a) Discuss the conversion strategies, Direct changeover, and Gradual conversion in brief.
(b) Discuss Operation evaluation in brief.

Design of Computerized Commercial Applications

15. Write a short note on 'Share Accounting'.

Enterprise Resource Planning: Redesigning Business

16. (a) Give some of the benefits achieved by implementing the ERP packages.
(b) What is Enterprise controlling? Also explain its three modules.

Controls in EDP Set-Up: General Controls

17. (a) Discuss the threats to operating system integrity.
(b) Explain various steps carried out under recovery plan.
18. Explain the special characteristics of Personal Computers (PC's), and their new security risks. Also explain the security measures that could be exercised for the same.

Controls in EDP Set-Up: Application Controls

19. (a) Discuss the control procedures to be implemented by organizations over source documents to account for each document.
(b) Explain the different classes and types of Transcription errors in brief.

Detection of Computer Frauds

20. (a) Define computer fraud with the help of some examples.
(b) Explain the steps which can be taken to detect fraud as soon as possible.

PAPER- 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

Cyber Laws and Information Technology Act (Amendment) 2008

21. Define the following terms with respect to information Technology (Amended) Act, 2008:

- (i) Digital signature
- (ii) Key pair
- (iii) Originator
- (iv) Secure system
- (v) Verify

Audit of Information Systems

22. (a) Explain the factors because of which, audit methods that are effective for manual audits prove ineffective in many IS audits.
- (b) Discuss the concurrent audit techniques used by the auditors.

Information Security

23. (a) Discuss 'Accountability' and 'Awareness' as the major principles of information security.
- (b) Discuss the subject areas covered by security standards, measures, practices, and procedures.
24. (a) Describe the issues that need to be addressed in achieving effective monitoring.
- (b) Write the names of the key controls of BS7799.

Use of Simple CASE Tools, Analysis of Financial Statements using Digital Technology

25. (a) Discuss the Analysis and design work benches in brief.
- (b) Explain different levels of data integration with reference to CASE Tools.

SUGGESTED ANSWERS / HINTS

1. (a) **Stress:** This is a force transmitted by a system's supra-system that causes a system to change, so that the supra-system can better achieve its goals. In trying to accommodate the stress, the system may impose stress on its subsystems, and so on.

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

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

FINAL (OLD) EXAMINATION: NOVEMBER, 2010

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

- (b) **Expert systems:** These systems are designed to replace the need for a human expert. They are particularly important where expertise is scarce and therefore expensive. This is not 'number-crunching' software, but software that expresses knowledge in terms of facts and rules. This knowledge will be in a specific area, and therefore expert systems are not general, as are most decision support systems which can be applied to most scenarios; an expert system for oil drilling is not of much use in solving company taxation problems

While there may have been a progression from transaction processing systems, through management information systems, to decision-support and executive information systems, expert systems have arisen largely from academic research into artificial intelligence. The expert system should be able to learn, i.e. change or add new rules. They are developed using very different programming languages such as PROLOG which are referred to as fifth generation languages or expert systems shells which can make the process quicker and easier. It has been suggested that expert systems would be of greater use in the tactical and strategic level. This has been the case in banking, where expert systems scrutinize applications for loans, and lower level staff accepts the system's decision. This has replaced the somewhat subjective decision-making of more senior managers.

2. (i) **Transaction File:** A transaction file is a collection of transaction input data. Transaction files usually contain data that are of temporary rather than permanent interest.
- (ii) **Master File:** By contrast to a transaction file, a master file contains data that are of a more permanent or continuing interest.
- (iii) **Reference File:** A reference or table file contains data that are necessary to support data processing. Common examples of reference files used in data processing are payroll tax tables and master price lists.
3. (a) A manager may be required to perform following activities in an organization:
- Determination of organizational objectives and developing plans to achieve them,
 - Securing and organizing the human and physical resources so that these objectives could be accomplished,
 - Exercising adequate controls over the functions, and
 - Monitoring the results to ensure that accomplishments are proceeding according to plan.
- (b) **Characteristics of an effective MIS:** Important characteristic for an effective MIS are eight in number and are briefly discussed below:

PAPER- 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

- (i) **Management oriented:** It means that effort for the development of the information system should start from an appraisal of management needs and overall business objectives. Such a system is not necessarily for top management only; it may also meet the information requirements of middle level or operating levels of management as well.
- (ii) **Management directed:** Because of management orientation of MIS, it is necessary that management should actively direct the system's development efforts. Mere one time involvement is not enough. For system's effectiveness, it is necessary for management to devote their sufficient time not only at the stage of designing the system but for its review as well, to ensure that the implemented system meets the specifications of the designed system. In brief, management should be responsible for setting system specifications and it must play a key role in the subsequent trade off decisions that occur in system development.
- (iii) **Integrated:** Development of information should be an integrated one. It means that all the functional and operational information sub-system should be tied together into one entity. An integrated information system has the capability of generating more meaningful information to management. The word integration here means taking a comprehensive view or a complete look at the interlocking sub-systems that operate within a company.
- (iv) **Common data flows:** It means the use of common input, processing and output procedures and media whenever possible is desirable. Data is captured by system analysts only once and as close to its original source as possible. They, then, try to utilize a minimum of data processing procedures and sub-systems to process the data and strive to minimize the number of output documents and reports produced by the system. This eliminates duplication in data collections and documents and procedures. It avoids duplication, also simplifies operations and produces an efficient information system. However, some duplication is necessary in order to insure effective information system.
- (v) **Heavy planning element:** An MIS usually takes 3 to 5 years and sometimes even longer period to get established firmly within a company. Therefore, a heavy planning element must be present in MIS development. It means that MIS designer should keep in view future objectives and requirements of firm's information in mind. The designer must avoid the possibility of system obsolescence before the system gets into operation.
- (vi) **Sub system concept:** Even though the information system is viewed as a single entity, it must be broken down into digestible sub-systems which can be implemented one at a time by developing a phasing plan. The breaking down of MIS into meaningful sub-systems sets the stage for this phasing plan.
- (vii) **Common database:** Database is the mortar that holds the functional systems together. It is defined as a "superfile" which consolidates and integrates data

FINAL (OLD) EXAMINATION: NOVEMBER, 2010

records formerly stored in many separate data files. The organization of a database allows it to be accessed by several information sub-systems and thus, eliminates the necessity of duplication in data storage, updating, deletion and protection. Although it is possible to achieve the basic objectives of MIS without a common database, thus paying the price of duplicate storage and duplicate file updating, database is a definite characteristic of MIS.

(viii) **Computerized:** It is possible to have MIS without using a computer. But use of computers increases the effectiveness of the system. In fact, its use equips the system to handle a wide variety of applications by providing their information requirements quickly. Other necessary attributes of the computer to MIS are accuracy and consistency in processing data and reduction in clerical staff. These attributes make computer a prime requirement in management information system.

4. (a) **Evaluation of MIS:** An effective MIS should be capable of meeting the information requirements of its executives in future as well. This capability can be maintained by evaluating the MIS and taking appropriate timely action. The evaluation of MIS should take into account the following points.

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

(b) **Limitations of MIS:** The main limitations of MIS are as follows:

- The quality of the outputs of MIS is basically governed by the quantity of input and processes.
- MIS is not a substitute for effective management. It means that it cannot replace managerial judgement in making decisions in different functional areas. It is merely an important tool in the hands of executives for decision making and problem solving.
- MIS may not have requisite flexibility to quickly update itself with the changing needs of time, especially in fast changing and complex environment.
- MIS cannot provide tailor-made information packages suitable for the purpose of every type of decision made by executives.
- MIS takes into account mainly quantitative factors, thus it ignores the non-quantitative factors like morale and attitude of members of the organization, which have an important bearing on the decision making process of executives.

PAPER- 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

- MIS is less useful for making non-programmed decisions. Such types of decisions are not of the routine type and thus require information, which may not be available from existing MIS to executives.
- The effectiveness of MIS is reduced in organizations, where the culture of hoarding information and not sharing with other holds.
- MIS effectiveness decreases due to frequent changes in top management, organizational structure and operational team.

5. (a) **Steps in the process of decision making:** These steps are given as follows:

- Perception or identification of decision problem,
- Diagnosis and definition of the decision problem,
- Specification of objectives,
- Collection of relevant information,
- Search for alternative courses of action,
- Evaluation of alternative courses of action,
- Making the final choice, and
- Implementation of the decision.

(b) **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 & 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 objective.
- (iv) **Profit Planning:** Financial decision concerning profits and dividends are to be taken by decision maker. S/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

FINAL (OLD) EXAMINATION: NOVEMBER, 2010

benefit of business. The purpose of tax planning is to take full advantage of exemptions, deductions, concessions, rebates, allowances and other reliefs.

- (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 organization.
 - (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.
6. (a) **Information required by a marketing system:** The information required for the purpose of planning in the case of a marketing system can be classified into three broad types:
- (i) **Environment information:** This information required for developing a Marketing System includes following:
 - a. *Political and governmental considerations:* To forecast market plans, information regarding political stability at any level i.e., at Centre or State; national or international, plays a significant role. Political stability enables executives to guess quite accurately the policies of the government and thus it helps them to reduce the risk while formulating plans for future. Tax considerations, financial policies, the nature and extent of government control and their effects on the organization are few other important considerations which provide useful information for planning purposes.
 - b. *Demographic and social trends:* Information about demography, its composition and location is also useful to business organization for planning its products, services or outputs.
 - c. *Economic trends:* This includes information related to the GNP level and trend, disposable income of consumers, employment, productivity, capital investment, price and wage levels, governmental economic priorities and numerous other economic indicators which provide valuable planning information for those firms whose output is function of these important variables.
 - (ii) **Competitive information:** Data relating to business operations of competing firms is quite useful for forecasting individual firm's product demand and making decisions and plans to achieve the forecast.
 - (iii) **Internal information:** The information available from internal sources is more important than the external one as it affects the planning decisions at different levels in the organization. The main sources of internal information are:
 - a. *Sales forecast:* It provides information about firm's sales plan. It sets the framework on which most of the internal plans are dependent.

PAPER- 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

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

Information required for the purpose of control is different in both type and characteristic from information needed for planning. Planning places greater emphasis on structuring the future, control is based more on the immediate past and specific trends. In the case of a marketing system, the information required for the purpose of control are information concerning the progress of the sales plan, quotas, territories, pricing etc. In other words the information required is meant to measure performance against the sales forecast. In addition, control information may be obtained in other areas of the marketing plan, such as product acceptance, advertising, market research and distribution costs.

- (b) The personnel system should be organized on functional basis. It should have the following information sub-systems to increase the operational efficiency of personnel management.
 - (i) **Recruitment:** Properly managed recruitment sub-system may forecast personnel needs and skills required for recruiting personnel at the proper time to meet organizational manpower needs. Such a sub-system may not only furnish information concerning skills required for company programmes and processes but also maintains the inventory of skills available within the organization.
 - (ii) **Placement:** This sub-system is concerned with the task of matching the available persons with the requirements. A good placement sub-system makes use of latest behavioral tools and techniques. It ensures that the capabilities of people are identified before being matched with properly organized work requirements.
 - (iii) **Training and development:** As technological changes and demands for new skills accelerate, many companies find that they must develop much of their requirements from internal sources. In addition, a large part of the workforce must constantly be updated in new techniques and developments. This task is the function of the training and development sub-system.
 - (iv) **Compensation:** This sub-system is concerned with the task of determining pay and other benefits for the workers of the concern. It makes use of traditional payroll and other financial records, government reports and unions expectation before arriving at the final figure of pay and other benefits for each category of workers.

FINAL (OLD) EXAMINATION: NOVEMBER, 2010

- (v) **Maintenance:** This sub-system is designed to ensure that personnel policies and procedures are achieved. It may be extended to the operation of systems control, work standards which are required to measure performance against financial plans or other programs, and the many subsidiary records normally associated with the collection, maintenance and dissemination of personnel data.
- (vi) **Health & Safety:** This sub-system is concerned with the health of personnel and the safety of jobs in the organization.

7. (a) Purpose of Executive Information System: These are stated below :

- (i) The primary purpose of an Executive Information System is to support managerial learning about an organization, its work processes, and its interaction with the external environment. Informed managers can ask better questions and make better decisions.
- (ii) A secondary purpose for an EIS is to allow timely access to information. All of the information contained in an EIS can typically be obtained by a manager through traditional methods. However, the resources and time required to manually compile information in a wide variety of formats, and in response to ever changing and ever more specific questions usually inhibit managers from obtaining this information. Often, by the time a useful report can be compiled, the strategic issues facing the manager have changed, and the report is never fully utilized.

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

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

The powerful focus of an EIS is due to the saying "what gets measured gets done." Managers are particularly attentive to concrete information about their performance when it is available to their superiors. This focus is very valuable to an organization if the information reported is actually important and represents a balanced view of the organization's objectives.

PAPER- 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

Misaligned reporting systems can result in inordinate management attention to things that are not important or to things which are important but to the exclusion of other equally important things. For example, a production reporting system might lead managers to emphasize volume of work done rather than quality of work. Worse yet, productivity might have little to do with the organization's overriding customer service objectives.

(b) A practical set of principles to guide the design of measures and indicators to be included in an EIS is presented below

- EIS measures must be easy to understand and collect. Wherever possible, data should be collected naturally as part of the process of work. An EIS should not add substantially to the workload of managers or staff.
- EIS measures must be based on a balanced view of the organization's objective. Data in the system should reflect the objectives of the organization in the areas of productivity, resource management, quality and customer service.
- Performance indicators in an EIS must reflect everyone's contribution in a fair and consistent manner. Indicators should be as independent as possible from variables outside the control of managers.
- EIS measures must encourage management and staff to share ownership of the organization's objectives. Performance indicators must promote both team-work and friendly competition. Measures will be meaningful for all staff; people must feel that they, as individuals, can contribute to improving the performance of the organization.
- EIS information must be available to everyone in the organization. The objective is to provide everyone with useful information about the organization's performance. Information that must remain confidential should not be part of the EIS or the management system of the organization.
- EIS measures must evolve to meet the changing needs of the organization.

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

- (i) Client/server architecture consists of a client process and a server process that can be distinguished from each other.
- (ii) The client portion and the server portions can operate on separate computer platforms.
- (iii) Either the client platform or the server platform can be upgraded without having to upgrade the other platform.
- (iv) The server is able to service multiple clients concurrently; in some client/server systems, clients can access multiple servers.

FINAL (OLD) EXAMINATION: NOVEMBER, 2010

- (v) The client/server system includes some sort of networking capability.
- (vi) A significant portion of the application logic resides at the client end.
- (vii) Action is usually initiated at the client end, not the server end.
- (viii) A user-friendly graphical user interface (GUI) generally resides at the client end.
- (ix) A structured query language (SQL) capability is characteristic of the majority of client/ server systems.
- (x) The database server should provide data protection and security.

(b) Client/server Risks and Issues

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

- **Technological Risks:** The technological risk is quite simple- Will the new system work? The short-term aspect of this question is -will it literally work? But more important is the risk that in the long run the system may grow obsolete. That it will become obsolete is probably inevitable thus the question becomes-how soon will it become obsolete. To resolve this issue the firm and the IT consultant/division should understand system standards and market trends and use them in their decision making processes while deciding what system to incorporate into their organization.
- **Operational Risks:** These risks parallel the technological risks in both the short and long run. Respectively, they are: will you achieve the performance you need from the new technology and will the software that you chose be able to grow or adapt to the changing needs of the business. Once again sound planning and keeping an eye to the future are the only remedies for these risks.
- **Economic Risks:** In the short run, firms are susceptible to hidden costs associated with the initial implementation of the new client/server system. Cost will rise in the short term since one needs to maintain the old system (mainframe) and the new client server architecture development. In the long run, the concern centers around the support costs of the new system.
- **Political Risks:** Finally, political (people) risks involved in this transition are addressed. Here, the short-term question is-will end users and management be satisfied? The answer to this is definitely not if the system is difficult to use or is plagued with problems.

9. (a) Disadvantages of Prototyping: Major disadvantages of this approach are as follows:

- Prototyping can only be successful if the system users are willing to devote significant time in experimenting with the prototype and provide the system

PAPER- 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

developers with change suggestions. The users may not be able or willing to spend the amount of time required under the prototyping approach.

- The interactive process of prototyping causes the prototype to be experimented with quite extensively. Because of this, the system developers are frequently tempted to minimize the testing and documentation process of the ultimately approved information system. Inadequate testing can make the approved system error-prone, and inadequate documentation makes this system difficult to maintain.
- Prototyping may cause behavioral problems with system users. These problems include dissatisfaction by users if system developers are unable to meet all user demands for improvements as well as dissatisfaction and impatience by users when they have to go through too many interactions of the prototype.

In spite of above listed limitations, to some extent, systems analysis and development has been greatly improved by the introduction of prototyping. Prototyping enables the user to take an active part in the systems design, with the analyst acting in an advisory role. Prototyping makes use of the expertise of both the user and the analyst, thus ensuring better analysis and design, and prototyping is a crucial tool in that process.

(b) There are many advantages to end-user computing, but there are also a number of risks involved. These risks include the following:

- A decline in standards and controls. When an analyst is in-charge of developments, walk-through will be done and standards and policies will be enforced; these things are unlikely to be carried out to the same degree with end-user computing.
- Inaccuracy of specification requirements. The end-user will not have the experience of an analyst in completing an accurate specification of system requirements.
- Due to the lack of adequate specifications, there would be a reduction in the quality assurance and stability of the system.
- An increase in unrelated and incompatible systems. Departments would choose their own software and hardware and incompatibility of systems would result; this would mean that management would have difficulty in obtaining full corporate data.
- 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.

10. (a) **Accountants' involvement in development work:** Most accountants are uniquely qualified to participate in systems development because they may be among the few people in an organization who can combine knowledge of IT, business,

FINAL (OLD) EXAMINATION: NOVEMBER, 2010

accounting, and internal control, as well as behaviour and communications, to ensure that new systems meet the needs of the user and possess adequate internal controls. They have specialized skills - such as accounting and auditing - that can be applied to the development project. For example, an accountant might perform the analysis of a proposed system's costs and benefits.

As internal, Information Technology (IT), and independent auditors, accountants provide a unique- and independent -perspective with which to evaluate the systems development process and the systems being developed.

(b) The analyst working on the preliminary investigation should accomplish the following objectives:

- **Clarify and understand the project request:** What is presently being done? What is required and why? Is there an underlying reason different from the one the user has identified?
- **Determine the size of the project:** Does a request for a project call for new development or for modification of the existing system? The investigation to answer this question will also gather the details useful in estimating the amount of time and number of people required to develop the project.
- Determine the technical and operational feasibility of alternative approaches.
- **Assess costs and benefits of alternative approaches:** What is the estimated cost for developing a particular system? Will the proposed system reduce operating costs? Will the proposed system provide better services to customers, etc?
- Report findings to the management with recommendation outlining the acceptance or rejection of the proposal.

11. (a) **Schedule Feasibility:** Schedule feasibility involves the design team's estimating how long it will take a new or revised system to become operational and communicating this information to the steering committee. For example, if a design team projects that it will take 16 months for a particular system design to become fully functional, the steering committee may reject the proposal in favour of a simpler alternative that the company can implement in a shorter time frame.

Legal Feasibility: Legal feasibility is largely concerned with whether there will be any conflict between a newly proposed system and the organization's legal obligations. For example, a revised system should comply with all applicable federal and state statutes about financial reporting requirements, as well as the company's contractual obligations.

(b) *Operating costs* of a computer based information system include:

- (i) hardware/software rental or depreciation charges,
- (ii) salaries of computer operators and other data processing personnel who will operate the new system,

PAPER- 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

- (iii) salaries of system analysts and computer programmers who perform the system maintenance function,
 - (iv) cost of input data preparation and control,
 - (v) cost of data processing supplies,
 - (vi) cost of maintaining proper physical facilities including power, light, heat, air conditioning, building rental or other facility charges and equipment and building maintenance charges, and
 - (vii) overhead charges of the business firm.
12. (a) 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 displays 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 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. Figure -5 shows a good placement of this information on the screen. The headings and titles are positioned at the top portion of the screen, messages and instructions at the bottom, and explanations if needed, on the right-hand side. If only a very small amount of information is to be presented, it can be placed in the centre of the screen or in the upper left quadrant. However, it is mainly a matter of preference of the concerned system analysts.

- (b) Some of the desired characteristics of a good coding scheme are enumerated below:
- (i) **Individuality:** The code must identify each object in a set uniquely and with absolute precision. To use one code number for several objects in a set would

FINAL (OLD) EXAMINATION: NOVEMBER, 2010

obviously cause a great deal of confusion. Furthermore, the code should be universally used over the entire organization.

- (ii) **Space:** As far as possible a code number must be much briefer than description.
- (iii) **Convenience:** The formats of code numbers should facilitate their use by people. This implies that the code number should be short and simple and consist of digits and or upper case alphabets. It is better to avoid the use of such special symbols as hyphens, oblique, dot, etc.
- (iv) **Expandability:** As far as possible future growth in the number of objects in a set should be provided for. Therefore, whilst introducing the scheme, longer number of digits/number than necessary at present may be adopted as the code length.

Related items must use fundamentally similar numbers. As an example, the pattern number, the casting number and the finished part number of a component at various stages of processing should have code numbers which mostly resemble but for a digits/letters alteration to suggest whether it is a pattern, casting or finished part. This is quite convenient when, for example, cross indexing which casting has to be ordered on the boundary for a particular part.

- (v) **Suggestiveness:** The logic of the coding scheme should be readily understandable. Also, the letter or number should be suggestive of the item characteristics e.g., whether it made from a casting or rolled stock, whether it pertains specifically to such and such model or it is used commonly by more than one end product. But this should not be carried too far in lengthening the code since it would defeat the purpose of brevity.
- (vi) **Permanence:** Changing circumstances should not invalidate the scheme or invalidation in the future should be kept to minimal.

13. (a) The following factors have to be considered towards rigorous evaluation:

- **The Performance Capability of Each Proposed System in Relation to its Costs:** It is imperative that a vendor system be capable of processing the organization's data within the time frames desired by management. Otherwise, delays in providing needed outputs will occur once the computer system is operational. There are many measures of performance, including speed, response time, number of users supported, and system testing. One way to examine the operating efficiency of a particular system is to use a benchmark test. With this approach, the vendor's system performs a data processing task that the new system must perform (e.g., payroll processing), and representatives of the organization then examine the outputs for accuracy, consistency, and efficiency.

PAPER- 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

- **The Costs and Benefits of Each Proposed System:** The accountants on the design team will analyze the costs of every vendor's proposed system in relation to the system's anticipated performance benefits – i.e., they will perform a cost-benefit analysis for each proposed system. In this effort, the accountants should also investigate the differences between purchasing and leasing each vendor's system. If the steering committee elects to purchase its computer system, the accountants should then advise the committee on a realistic depreciation schedule for the new system.
 - **The Maintainability of Each Proposed System:** Maintainability refers to the ease with which a proposed computer system can be modified. For example, this flexibility enables a firm to alter a portion of a payroll system to reflect new federal tax laws. Because the costs of maintaining a large information system are typically five times as much as the costs of initially acquiring or developing a system, the evaluators should place considerable emphasis on this dimension.
 - **The Compatibility of Each Proposed system with Existing Systems:** Compatibility refers to the ability to implement and interface the new system with existing computer resources and software. In some instances, this comes down to hardware issues. For example, it may not be possible to run specific software modules of the new system on some of the company's older local area network servers, which will consequently have to be upgraded. But compatibility issues can also involve the operating system, existing application software, or procedural concerns as well – for example, the requirement that employees learn a whole new set of procedures for inputting data.
 - **Vendor Support:** Vendor support includes such things as (1) training classes that familiarize employees with the operating characteristics of the new system, (2) help in implementing and testing the new system, (3) assistance in maintaining the new system through a maintenance contract, and (4) backup systems for temporarily processing company data if required. The availability of "business-hours-only" versus "round-the-clock" support is another consideration. Most vendors charge extra for enhanced services.
- (b) **Examples of Support Service Checklists:** Some examples are given as follows:
- *Performance:* What has been the vendor's past performance in terms of his past promises?
 - *System development:* Are system analysis and programming consultants available? What are their qualities and cost?
 - *Maintenance:* Is equipment maintenance provided? What is the quality and cost?
 - *Conversion:* What systems development, programming and hardware installation service will they provide during the conversion period?

FINAL (OLD) EXAMINATION: NOVEMBER, 2010

- *Training:* Is the necessary training of personnel provided? What is its quality and cost?
- *Back-up:* Are several similar computer facilities available for emergency back up purposes?
- *Proximity:* Does the vendor have a local office? Are sales, systems development, programming, and hardware maintenance services provided from the office?
- *Hardware:* Do they have a wide selection of compatible hardware?
- *Software:* Do they have a wide variety of useful systems software application programs?

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

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

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

Gradual conversion: Gradual conversion attempts to combine the best features of the earlier two plans, without incurring the risks. In this plan, the volume of transactions is gradually increased as the system is phased in. The advantages include allowing users to get involved with the system gradually and the possibility of detecting and recovering from the errors without a lot of downtime. Disadvantages of gradual conversion include taking too long to get the new system in place and its inappropriateness for conversion of small, uncomplicated systems.

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

- Are all transactions processed on time?
- Are all values computed accurately?
- Is the system easy to work with and understand?
- Is terminal response time within acceptable limits?
- Are reports processed on time?

PAPER- 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

- Is there adequate storage capacity for data?

Operation evaluation is relatively straightforward if evaluation criteria are established in advance. For example, if the systems analyst lays down the criterion that a system which is capable of supporting one hundred terminals should give response time of less than two seconds, evaluation of this aspect of system operation can be done easily after the system becomes operational.

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

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

When a person purchases shares from a share holder, a share transfer form along with the certificates is sent by the buyer to the company for incorporating the transfer. The system records a change in ownership for the shares from the seller to the buyer.

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

Other facilities usually provided in share accounting system are :

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

Main *inputs* in a share accounting system are:

- shareholding data from a fresh issue-this is usually supplied by the issue agency on electronic media
- share transfer request
- split request
- consolidation request
- request for bank mandate
- tax exemption forms

FINAL (OLD) EXAMINATION: NOVEMBER, 2010

- request for duplicate certificates
- request for duplicate dividend warrants
- change in shareholder's address.

Processing involves:

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

Main outputs are:

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

16. (a) The benefits achieved by implementing ERP packages are given as follows:
- Gives Accounts Payable personnel increased control of invoicing and payment processing and thereby boosting their productivity and eliminating their reliance on computer personnel for these operations.
 - Reduce paper documents by providing on-line formats for quickly entering and retrieving information.
 - Improves timeliness of information by permitting posting daily instead of monthly.
 - Greater accuracy of information with detailed content, better presentation, satisfactory for the auditors.
 - Improved cost control.
 - Faster response and follow-up on customers.
 - More efficient cash collection, say, material reduction in delay in payments by customers.
 - Better monitoring and quicker resolution of queries.
 - Enables quick response to change in business operations and market conditions.
 - Helps to achieve competitive advantage by improving its business process.
 - Improves supply-demand linkage with remote locations and branches in different countries.
 - Provides a unified customer database usable by all applications.

PAPER- 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

- Improves International operations by supporting a variety of tax structures, invoicing schemes, multiple currencies, multiple period accounting and languages.
 - Improves information access and management throughout the enterprise.
 - Provides solution for problems like Y2K and Single Monetary Unit (SMU) or Euro Currency.
- (b) **Enterprise Controlling:** Enterprise can be managed by using an Integrated Enterprise Management. This consists of getting accounting data prepared by subsidiaries for corporate reporting which will be automatically prepared simultaneously within the local books of each subsidiary. This data is transferred to a module called Enterprise Controlling (EC).

It is easy to transfer the data to the EC module to automatically set up consolidated financial statements including elimination of inter-company transactions, currency translation etc.

Enterprise Controlling consists of following three modules:

- (i) **EC-CS:** This component is used for financial statutory and management consolidation which also allows fully automated consolidation of investments-even for many companies and complex investment structures.
- (ii) **EC-PCA:** Allows to work with internal transfer prices and at the same time to have the right values from company, profit centre, and enterprise perspectives in parallel. Any transaction that touches an object such as customer order, plant or cost centre allocated to a profit centre will be automatically posted to EC-PCA.

It is also possible to take data directly from EC-PCA to EC-CS consolidation to prepare complete financial statutory statements and management reports in parallel. This provides the management with a consistent view of external and internal financial management reports.

- (iii) **EC-EIS (Executive Information System):** Executive Information System allows to take financial data from EC-PCA ,EC-CS or any other application and combine with any external data such as market data, industry benchmarks and /or data from non-SAP applications to build a company specific comprehensive enterprise information system .

Enterprise Controlling allows to control the whole enterprise from a corporate and a business unit perspective within one common infrastructure. It helps to speed up provision of business control information by fully automated corporate reporting from operative accounting via financial consolidation to management reporting.

From EC-EIS top-level reports, end users can drill down to more detailed information within EC or any other R/3 application.

FINAL (OLD) EXAMINATION: NOVEMBER, 2010

EC can work with data from SAP and non-SAP sources.

17. (a) **Threats to Operating System Integrity:** Operating system control objectives are sometimes not achieved because of flaws in the operating system that are exploited either accidentally or intentionally.

Accidental threats include hardware failures that cause the operating system to crash. Operating system failures are also caused by errors in user application programs that the operating system cannot interpret. Accidental system failures may cause whole segments of memory to be “dumped” to disks and printers, resulting in the unintentional disclosure of confidential information.

Intentional threats to the operating system are most commonly attempts to illegally access data or violate user privacy for financial gain. However, a growing form of threat is from destructive programs from which there is no apparent gain. These exposures come from three sources:

- Privileged personnel who abuse their authority. Systems administrators and systems programmers require unlimited access to the operating system to perform maintenance and to recover from system failures. Such individuals may use this authority to access users' programs and data files.
- Individuals, both internal and external to the organization, who browse the operating system to identify and exploit security flaws.
- An individual who intentionally (or accidentally) inserts a computer virus or other form of destructive program into the operating system.

- (b) The following steps may be carried out under this plan:

- (i) An inventory of the hardware, application systems, system software, documentation etc. must be taken.
- (ii) Criticality of application systems to the organization and the importance of their loss must be evaluated. An indication must be given of the efforts and cost involved in restoring the various application systems.
- (iii) An application systems hierarchy must be spelt out. This would be used when the management decides to accept a degraded mode of operation.
- (iv) Selection of a disaster recovery site must be made. A reciprocal agreement with another organisation having compatible hardware and software could be made. However, systems availability and data security problems must be considered at this point. Hiring a service bureau is another option. If the situation warrants, a fully operational backup site could also be considered.
- (v) A formal backup agreement with another company must be made. This should cover the periodical exchange of information between the two sites regarding changes to hardware/software, the time and duration of systems availability, modalities of testing the plan etc.

PAPER- 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

18. The capabilities, adaptability and user friendliness of Personal Computers (PC's) are posing a serious challenge to auditors. PC's have the following special characteristics which give rise to new risks.

- They are small, fast, and powerful. Some of them even approach the power of minis and mainframes.
- They are available in many makes and models.
- Floppies provide a convenient way of data storage.
- Their user – friendliness has resulted in end–user computing.
- They act as inexpensive front–ends to larger computers.
- There is a tendency to buy off–the shelf application packages.
- They are prone to virus infection.

The resultant new security risks are as follows:

- PC's are likely to be shifted from one location to another or even taken outside the organization.
- Decentralized purchasing of PC's can result in hardware/software incompatibility in the long run.
- Floppies can be very conveniently transported from one place to another, as a result of which data corruption may occur. Mishandling, improper storage etc. can also cause damage.
- The inherent data security provided is rather poor.
- There is a chance that applications software are not thoroughly tested.
- Segregation of duties is not possible, owing to limited number of staff.
- The operating staff may not be adequately trained.
- Computer viruses can slow down the system, corrupt data and so on.

The security measures that could be exercised are as follows:

- Physically locking the keyboard or the PC itself must be enforced.
- Proper logging of equipment shifting must be done.
- The PC purchases must be centrally coordinated and company-wide standards established for spread sheets, word-processors, applications software etc.
- Floppies must be stored in secured places and their issues duly authorized. They must be adequately packed before any shipment.
- Data and programs on hard-disks must be secured using hardware/software mechanisms. Backups must be taken regularly.

FINAL (OLD) EXAMINATION: NOVEMBER, 2010

- Minimum standards must be set for developing, testing and documenting applications.
 - Properly organized training programs must be periodically conducted. More than one user should be trained on each application.
 - Virus prevention and detection software obtained from reliable sources must be used. Write protect tabs should be used on diskettes that do not require any alteration. Pirated software should be strictly avoided.
 - The PC's and their peripherals must be maintained regularly.
 - While the proliferation of powerful PC's in recent years has its own plus points, the associated risks must not be ignored. Thus, implementing effective controls is of prime importance.
19. (a) The organization must implement control procedures over source documents to account for each document, as described below.
- *Use Pre-numbered Source Documents:* Source documents should come pre-numbered from the printer with a unique sequential number on each document. Source document numbers permit accurate accounting of document usage and provide an audit trail for tracing transactions through accounting records.
 - *Use Source Documents in Sequence:* Source documents should be distributed to the users and used in sequence. This requires that adequate physical security be maintained over the source document inventory at the user site. When not in use, documents should be locked away. At all times, access to source documents should be limited to authorized persons.
 - *Periodically Audit Source Documents:* Missing source documents should be identified by reconciling document sequence numbers. Periodically, the auditor should compare the numbers of documents used to date with those remaining in inventory plus those voided due to errors. Documents not accounted for should be reported to management.
- (b) Transcription errors fall into three classes:
- (i) *Addition errors* occur when an extra digit or character is added to the code. For example, inventory item number 83276 is recorded as 832766.
 - (ii) *Truncation errors* occur when a digit or character is removed from the end of a code. In this type of error, the inventory item above would be recorded as 8327.
 - (iii) *Substitution errors* are the replacement of one digit in a code with another. For example, code number 83276 is recorded as 83266.

There are two types of transposition errors. *Single transposition errors* occur when two adjacent digits are reversed. For instance, 83276 is recorded as 38276. *Multiple transposition errors* occur when nonadjacent digits are transposed. For example, 83276 is recorded as 87236.

PAPER- 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

Any of these errors can cause serious problems in data processing if they go undetected. For example, a sales order for customer 732519 that is transposed into 735219 will be posted to the wrong customer's account. A similar error in an inventory item code on a purchase order could result in ordering unneeded inventory and failing to order inventory that is needed. These simple errors can severely disrupt operations.

20. (a) Computer frauds have been defined as any illegal act for which knowledge of computer technology is essential for its perpetration, investigation or prosecution. Most specifically, computer frauds include the following:
- Unauthorized theft, use, access, modification, copying and destruction of software or data
 - Theft of money by altering computer records or the theft of computer time
 - Theft or destruction of computer hardware
 - Use or the conspiracy to use computer resources to commit an offence
 - Intend to illegally obtain information or tangible property through the use of computer
- (b) Many companies are currently being defrauded and do not know it. The following steps can be taken to detect fraud as soon as possible:
- (i) **Conduct Frequent Audits:** One way to increase the likelihood of detecting fraud and computer abuses is to conduct periodic external and internal audits as well as special network security audits. Auditors should regularly test system controls and periodically browse data files looking for suspicious activities. However, care must be exercised to make sure employees' privacy rights are not violated.
 - (ii) **Use a Computer Security Officer:** Most frauds are not detected by internal or external auditors. The study shows that assigning responsibility for fraud deterrence and detection to a computer security officer has a significant deterrent effect. This person should be independent of the information system function. The security officer can monitor the system and disseminate information about improper system uses and their consequences.
 - (iii) **Use Computer Consultants:** Many companies use outside computer consultants or in-house teams to test and evaluate their security procedures and that is detected is closely evaluated, and corresponding protective measures are implemented. Some companies dislike this approach, because neither they want their weaknesses to be exposed nor do they want their employees to know that the system can indeed be broken into.
 - (iv) **Monitor system Activities:** All system transactions and activities should be recorded in a log. The log should indicate who accessed what data, when, and from which terminal. These logs should be reviewed frequently to monitor system activity and trace any problems to their source.

FINAL (OLD) EXAMINATION: NOVEMBER, 2010

There are a number of risk analysis and management software packages that can review computer systems and networks. These systems evaluate security measures already in place and test for weaknesses and vulnerabilities. A series of reports is then generated that explain the weaknesses found and suggest improvements.

- (v) **Use Fraud Detection Software:** People who commit fraud tend to follow certain patterns and leave behind telltale clues, such as things that do not make sense. Software has been developed to search out these fraud symptoms.
21. (i) **Digital Signature:** It means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3.
- (ii) **Key Pair:** In an asymmetric crypto system, Key Pair means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key.
- (iii) **Originator:** This means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary.
- (iv) **Secure System:** This means computer hardware, software, and procedure that:
- (a) are reasonably secure from unauthorized access and misuse;
 - (b) provide a reasonable level of reliability and correct operation;
 - (c) are reasonably suited to performing the intended functions; and
 - (d) adhere to generally accepted security procedures.
- (v) **Verify:** “verify” in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether:
- (a) the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;
 - (b) the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.
22. (a) The audit methods that are effective for manual audits prove ineffective in many IS audits because of these factors:
- **Electronic evidence:** Essential evidence is not physically retrievable by most auditors, and it is not readable in its original electronic form.
 - **Terminology:** The tools and techniques used in automated applications are described in terms that are difficult for the non-EDP auditor to understand.
 - **Automated processes:** The methods of processing are automated rather than manual, making it difficult for the non-EDP auditor to comprehend processing concepts and the logic of these concepts.

PAPER- 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

- **New risks and controls:** Threats to computer systems and the countermeasures to those threats (i.e. controls) are new to non-EDP auditors, and the magnitude of the risks and the effectiveness of the controls are not understood.
- **Reliance 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.

Because the rate of these changes varies among systems in organizations, the methods and approaches of auditing automated information systems differ among applications and organizations. For example, some organizations still rely heavily on hard-copy evidence, and others have eliminated much of it.

(b) Auditors commonly use five concurrent audit techniques:

- (i) **An Integrated Test Facility (ITF)** technique places a small set of fictitious records in the master files. The records might represent a fictitious division, department, or branch office or a customer or supplier. Processing test transactions to update these dummy records will not affect the actual records. Because fictitious and actual records are processed together, company employees usually remain unaware that this testing is taking place. The system must distinguish ITF records from actual records, collect information on the effects of the test transactions, and report the results. The auditor compares processing and expected results in order to verify that the system and its controls are operating correctly.

In a batch processing system, the ITF technique eliminates the need to reverse test transactions and is easily concealed from operating employees. ITF is well suited to testing on-line processing systems because test transactions can be submitted on a frequent basis, processed with actual transactions, and traced throughout every processing stage. All this can be accomplished without disrupting regular processing operations. However, care must be taken not to combine dummy and actual records during the reporting process.

- (ii) **The snapshot technique** examines the way transactions are processed. Selected transactions are marked with a special code that triggers the snapshot process. Audit modules in the program record these transactions and their master file records before and after processing. Snapshot data are recorded in a special file and reviewed by the auditor to verify that all processing steps have been properly executed.
- (iii) **SCARF** (system control audit review file) uses embedded audit modules to continuously monitor transaction activity and collect data on transactions with special audit significance. The data are recorded in a SCARF file or **audit log**. Transactions that might be recorded in a SCARF file include those exceeding a specified rupee limit, involving inactive accounts, deviating from company

FINAL (OLD) EXAMINATION: NOVEMBER, 2010

policy, or containing write-downs of asset values. Periodically the auditor receives a printout of the SCARF file, examines the information to identify any questionable transactions, and performs any necessary follow-up investigation.

- (iv) **Audit hooks** are audit routines that flag suspicious transactions. For example, internal auditors at an Insurance Company determined that their policyholder system was vulnerable to fraud every time a policyholder changed his or her name or address and then subsequently withdrew funds from the policy. They devised a system of audit hooks to tag records with a name or address change. The internal audit department is now notified when a tagged record is associated with a withdrawal and can appropriately investigate the transaction for fraud. When audit hooks are employed, auditors can be informed of questionable transactions as soon as they occur. This approach, known as **real-time notification**, displays a message on the auditor's terminal.
- (v) **Continuous and intermittent simulation (CIS)** embeds an audit module in a data base management system. The CIS module examines all transactions that update the DBMS using criteria similar to those of SCARF. If a transaction has special audit significance, the module independently processes the data (in a manner similar to parallel simulation), records the results, and compares them with those obtained by the DBMS. If any discrepancies exist, the details are written onto an audit log for subsequent investigation. If serious discrepancies are discovered, the CIS may prevent the DBMS from executing the update process.

23. (a) **Accountability** - *Responsibility and accountability must be explicit.*

Security of information requires an express and timely apportionment of responsibility and accountability among data owners, process owners, technology providers, and users. This accountability should be formalized and communicated.

Issues to consider include:

- ◆ specification of ownership of data and information;
- ◆ identification of users and others who access the system in a unique manner;
- ◆ recording of activities through the provision of management audit trails;
- ◆ assignment of responsibility for maintenance of data and information; and
- ◆ institution of investigative and remedial procedures when a breach or attempted breach of the security objective occurs.

Awareness - *Awareness of risks and security initiatives must be disseminated.*

In order to foster confidence in information, data owners, process owners, technology providers, users, and other parties, with a legitimate interest to learn or be informed, must be able to gain knowledge of the existence and general extent of the risks facing the organization and its systems 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.

PAPER- 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

Issues to consider include:

- ◆ level of detail disclosed must not compromise security;
 - ◆ appropriate knowledge is available to all parties, not just users, who have a legitimate right to be informed;
 - ◆ awareness is part of the induction program for new recruits to an organization so as to build security awareness as part of the corporate culture; and
 - ◆ recognition that maintaining awareness is an on-going process.
- (b) The security standards, measures, practices, and procedures will cover a number of subject areas including:
- (i) *Managerial controls*, such as span of control, separation of duties, background checks, and personnel awareness, training, and education to ensure that personnel act appropriately to prevent, detect, or correct problems.
 - (ii) *Identification and authentication controls* to establish accountability and to prevent unauthorized persons from gaining access to the systems through, for example, passwords or smart tokens;
 - (iii) *Logical access controls* to establish who or what has access to a specific type of information resources and the type of access permitted, such as read, write, update, or delete;
 - (iv) *Accountability controls* through management audit trails that maintain a record of all user and system activity;
 - (v) *Cryptography Controls* over information transmitted and stored to ensure confidentiality, authenticity, integrity, and non-repudiation;
 - (vi) *Systems development life cycle process controls* to ensure that security is considered as an integral part of the process and explicitly considered during each phase of the process;
 - (vii) *Physical and environmental controls* (encompassing physical access, fire detection and prevention, air-conditioning and power supply continuity, structural soundness, and the physical security of data transmission lines) to ensure that adequate measures are taken against threats emanating from the physical environment;
 - (viii) *Computer support and operations controls* to ensure that these routine but critical activities (user support, software support, change management, configuration management, media controls, backups, documentation, and maintenance) enhance the overall level of security; and
 - (ix) *Business continuity planning controls* to ensure that an organization can prevent interruptions, and recover and resume processing in the event of a partial or total interruption to information systems availability.

24. (a) Issues that need to be addressed in achieving effective monitoring include:

FINAL (OLD) EXAMINATION: NOVEMBER, 2010

- the appointment of a responsible manager with adequate tools and resources;
- the performance of independent and objective assessments of security controls such as provided by security audits;
- the establishment of clear and expedient investigative procedures;
- the massive amount of management audit trail information from a large variety of system components that may need to be examined;
- the timeliness of escalation processes when electronic transactions are practically instantaneous; and
- the dynamic and ever changing business and information systems environment.

(b) Ten key Controls of BS7799 are given as follows:

- (i) Information security policy document
- (ii) Allocation of information security responsibilities
- (iii) Information Security Education & Training
- (iv) Reporting of Security Incidents
- (v) Virus Controls
- (vi) Business Continuity Planning Process
- (vii) Control of proprietary software copying
- (viii) Safeguarding of organizational records
- (ix) Data Protection
- (x) Compliance with security policy

25. (a) Analysis and design work benches : Analysis and design work benches are designed to support the analysis and design stages of the software process where models of the system are created. A typical model is shown in given figure. The components of this model are:

- (a) *Diagram editors* to create data flow diagrams, structured charts, entity relationship diagram and so on.
- (b) *Design analysis and checking tools* which process the design and then submit report on errors and anomalies. These are integrated with editing system so that user errors are trapped at an early stage in the process.
- (c) *Repository query languages* which allow the designer to find the designs and associate design information in the repository.
- (d) *A data dictionary* which maintains information about the entities used in a system design.
- (e) *Report definition and generation tools* which take information from the central store and automatically generate system documentation.

PAPER- 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

- (f) *Forms definition tools* which allow screen and document formats to be specified.
- (g) *Import-export facilities* which allow the interchange of information from the central repository with other development tools .
- (h) *Code generators* which generate code or code skeletons automatically from the design captured in the central store.

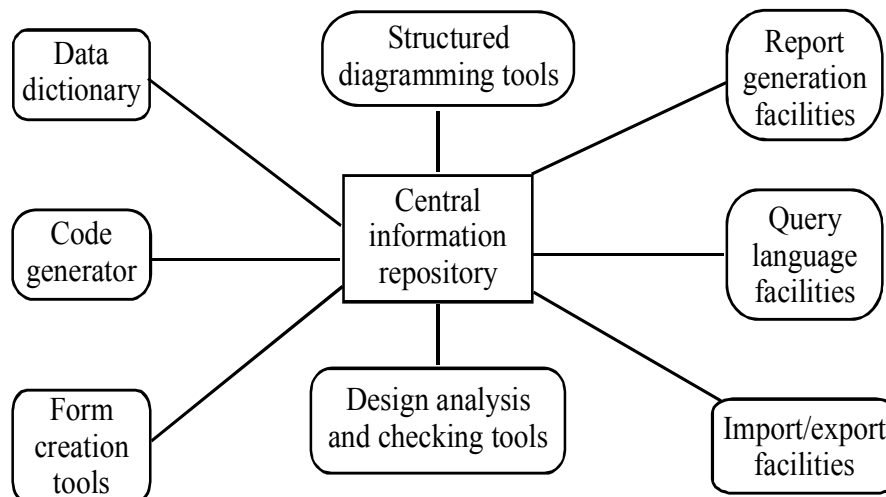


Figure: An Analysis and Design work bench

- (b) Data integration is the process of exchange of data by CASE tools. The result from one tool can be passed on as input to another tool. There are a number of different levels of data integration:
 - (a) *Shared files*: All tools recognize a single file format. The most general purpose shareable file format is where files are made of lines of characters.
 - (b) *Shared data structures*: The tools make use of shared data structures which usually include program or design language information. This is shown in figure.
 - (c) *Shared repository*: The tools are integrated around an object management system which includes a public share data model describing the data entities and relationships which can be manipulated by the tools.

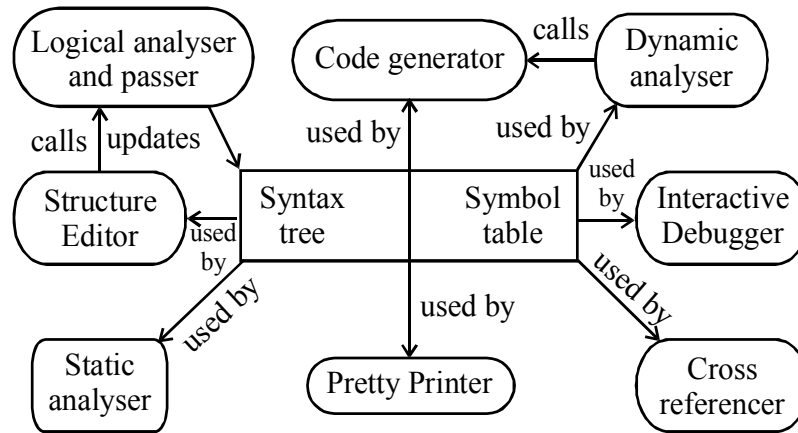


Figure: Integration through shared Data Structure