PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

QUESTIONS

**Note : The IT Act, 2000 has been amended. For details to IT Act (amended 2008), refer to the link http://www.icai.org/post.html?post_id=1056*

Basic Concepts of Systems

1. (a) Define systems and explain the general model of the system.

   (b) Differentiate between closed and open systems.

Transaction Processing Systems

2. Explain the four common cycles of a business activity.

Basic Concepts of MIS

3. (a) Examine the prerequisites of an effective MIS. What are the major constraints in operating an effective MIS?

   (b) What are the information requirements at the lower level for making decisions?

Systems Approach and Decision Making

4. (a) System analysts develop various categories of information systems to meet a variety of business needs. Discuss any three such systems briefly.

   (b) List out the benefits of successful materials requirement planning systems.

Decision Support and Executive Information Systems

5. (a) Trace the data flow representation of the executive decision-planning environment.

   (b) What are the set of principles that guide the design of measures and indicators to be included in an Executive Information System?

Enabling Technologies

6. (a) What are the control techniques that are essential for the security of the client/server environment?

   (b) What are the risks associated with client/server model?

System Development Process

7. (a) Read the data flow and activities listed in the table below carefully and draw the data flow diagram for the payroll processing system.

Activities	Data Inputs	Data Outputs
Update employee/roll file	New employee form Employee change form Employee/payroll file	Updated employee/ payroll file

Pay employees	Time cards Employee/ payroll file Tax tables	Employee cheques Payroll register Updated employee/payroll file Payroll cheques Payroll cash disbursements voucher
Prepare reports	Employee/ payroll file	Payroll report
Pay taxes	Employee/ payroll file	Tax report Tax payment Payroll tax cash disbursements voucher Updated employee/payroll file
Update general ledger	Payroll tax cash Disbursements voucher Payroll cash Disbursements voucher	Updated general ledger

(b) What is a data dictionary? What are its uses?

Systems Design

8. (a) What are the different formats in which information can be presented? Discuss briefly, the guidelines to be considered while designing a graphic format.

   (b) What is a system manual? What information is included in it?

System's Acquisition, Software Development and Testing

9. (a) Discuss in brief, salient features of consideration while selecting a computer system. Also suggest contents in a point scoring table for evaluation of a "ready to use software".

   (b) Briefly describe various steps involved in system testing.

Systems Implementation and Maintenance

10. (a) Explain strategies that can be adopted for converting an old information system to the new system.

    (b) Explain the role of system maintenance in the development of an Information system.

Design of Computerised Commercial Applications

11. (a) List out the various outputs of the Inventory control system.

(b) What is a share accounting system? List out the facilities provided in the share accounting system.

Enterprise Resource Planning: Redesigning Business

12. Explain the general model of the Enterprise Resource Planning.

13. (a) List out some of the entities forming a data model in business modelling.

(b) ABC company has presence across India in manufacturing of medicine. The management of the company intends to centralize and integrate the information flow across its different manufacturing units in a uniform manner at various levels of the company. Presently the company has its functioning at different units being automated as per the local requirements, technical expertise and on an ad-hoc basis. The technical advisor of the company recommends that the company should go for the implementation of the ERP Package. List out the reasons for ERP adoption by the company?

Controls in EDP Set-up: General Controls

14. Explain the various types of threats to operating system integrity.

15. Explain the role of insurance in covering residual risks that exist in the computer system.

16. How can the firewall control or avoid denial of service attacks?

Controls in EDP Set-up: Application Controls

17. Explain the three levels of input validation controls.

18. List out the various checks that can be performed during a validation run. Briefly explain the various types of Transaction checks.

Detection of Computer Frauds

19. (a) List out the various sources from where the information can be recovered to investigate computer frauds.

(b) What steps can be taken to detect computer fraud as soon as possible?

Cyber Laws and Information Technology Act 2000

20. Define some of the following terms as mentioned in Information Technology Act, 2008 (Amended):

(a) Asymmetric crypto system

(b) Electronic form

(d) Electronic record

(e) Electronic signature

(f) Electronic signature certificate

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

Audit of Information Systems

22. (a) What is the purpose of an IS audit? While performing an IS audit, what are the objectives to be ascertained by the Auditors.

    (b) Write briefly about Test Data Processing.

Information Security

23. (a) Briefly describe the objectives of information security policy.

    (b) Discuss various ways to protect computer held information.

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

24. (a) List out the various CASE tools with specific examples of each tool.

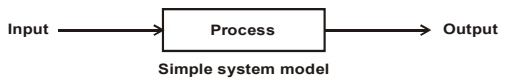
    (b) Explain the process of exchange of data by CASE tools.

25. Briefly explain the components of analysis and design work-bench.

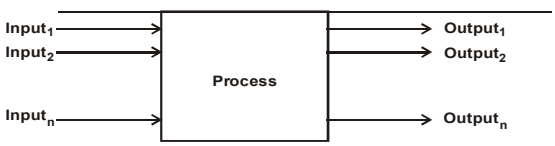
SUGGESTED ANSWERS/HINTS

1. (a) The term system may be defined as a set of interrelated elements that operate collectively to accomplish some common purpose or goal. A business is also a system where economic resources such as people, money, material, machines, etc are transformed by various organisational processes (such as production, marketing, finance etc.) into goods and services. A computer based information system is also a system which is a collection of people, hardware, software, data and procedures that interact to provide timely information to authorised people who need it.

Systems can be abstract or physical. An abstract system is an orderly arrangement of interdependent ideas or constructs. A physical system is a set of elements which operate together to accomplish an objective. A general model of a physical system is input, process and output. This is, of course, very simplified because a system may have several inputs and outputs as shown below:



Simple system model



System with many inputs and outputs

For details to above points, refer to study material, Chapter-1, Section 1.1.

(b) Closed and Open Systems: A Closed System is self-contained and does not interact or make exchange across its boundaries with its environment. Closed systems do not get the feedback they need from the external environment and tend to deteriorate. A Closed Systems is the one that has only controlled and well defined input and output. Participants in a closed system become closed to external feed back without fully being aware of it. Some of the examples of closed systems are manufacturing systems, computer programs etc.

Open System actively interact with other systems and establish exchange relationship. They exchange information, material or energy with the environment including random and undefined inputs. Open systems tend to have form and structure to allow them to adapt to changes in their external environment for survival and growth. Organisations are considered to be relatively open systems.

For details to above points, refer to study material, Chapter-1, Section 1.3.

2. The four common cycles of a business activity are:

(i) ***Revenue cycle:*** Events related to the distribution of goods and services to other entities and the collection of related payments. It involves processing cash sales, credit sales, and receipt of cash following a credit sale.

(ii) ***Expenditure cycle:*** Events related to acquisition of goods and services from other entities and the settlement of related obligations.

(iii) ***Production cycle:*** Events related to the transformation of resources into goods and services. It involves the planning, scheduling, and control of the physical product through the manufacturing process.

(iv) ***Finance cycle:*** Events related to the acquisition and management of capital funds, including cash. It might also include application systems concerned with cash management and control, debt management, and administration of employee benefit plans.

3. (a) The main prerequisites of an effective MIS are as follows:

(i) **Database:** It can be defined as a "superfile" which consolidates data records formerly stored in many data files. The data in a database is organized in such a way that access to the data is improved and redundancy is reduced. The characteristics of database are:

- The database is sub-divided into major information subsets needed to run a business wherein each subsystem utilizes same data and information kept in same file to satisfy its information needs.
- It is user-oriented.
- It is capable of being used as a common data source, to various users, helps in avoiding duplication of efforts in storage and retrieval of data and information.

- It is available to authorized persons only.
- It is controlled by a separate authority established for the purpose, known as Data Base Management System (DBMS).
- The maintenance of data in database requires computer hardware, software and experienced computer professionals.

(ii) **Qualified system and management staff:** The second prerequisite is that it should be manned by qualified officers. For this, the organisational management base should comprise of two categories of officers.

- Systems and Computer experts: They, in addition to their expertise in their subject area should be capable of understanding management concepts to facilitate the understanding of problems faced by the concern. They should also be clear about the process of decision making and information requirements for planning and control functions.
- Man*agement experts*: They should understand quite clearly the concepts and operations of a computer.

(iii) **Support of Top Management:** The management information system to be effective, should receive the full support of the top management. The reasons for this are as follows:

- Subordinate managers are usually lethargic about activities which do not receive the support of their superiors.
- The resources involved in computer-based information systems are large and are growing larger in view of importance gained by management information system.

(iv) **Control and Maintenance of MIS:** Control of the MIS means the operation of the system as it was designed to operate. Sometimes users develop their own procedures or short cut methods to use the system, which reduce its effectiveness. To check such habits of users, the management at each level in the organization should device checks for the information system control. At times, there may be the need for improvements to the system. Formal method and documenting always must be provided. Maintenance is closely related to control.

(v) **Evaluation of MIS:** 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.
- Guiding the appropriate authority about the steps to be taken to maintain effectiveness of MIS.

The major constraints which come in the way of operating a management information system are as follows:

(i) *Non-availability of experts*, who can diagnose the objectives of the organisation and provide a desired direction for installing and operating system. This problem may be overcome by grooming internal staff. The grooming of staff should be preceded by proper selection and training.

(ii) *Non availability of standard MIS product*. Experts usually face the problem of selecting the sub-system of MIS to be installed and operated upon.

(iii) *Non-availability of cooperation from staff*. Educating the staff may solve this problem. This task should be carried out by organizing lectures, showing films and also explaining to them the utility of the system. Besides this, some persons should also be involved in the development and implementation of the system.

(iv) *High turnover of experts in MIS*. Turnover in fact arises due to several factors like pay packet; promotion chances; future prospects, behaviour of top ranking managers etc. Turnover of experts can be reduced by creating better working conditions and paying at least at par with other similar concerns.

(v) *Difficulty in quantifying the benefits of MIS*, so that it can be easily comparable with cost. This raises questions by departmental managers about the utility of MIS.

For details to above points, refer to study material, Chapter-3 Section 3.1.5.

(b) The information requirements at lower level for making decisions are classified into two types.

(i) External Information

(ii) Internal Information

The information requirement at lower level for making decisions is given in the chart below:

External Information	Internal Information
Sensitive changes affecting material supplies and sales.	Unit sales and expenses. Current performances. Shortages and bottle-necks. Operating efficiencies and inefficiencies. Input-output ratios. Maintenance reports.

4. (a) Systems analysts develop the following types of information systems to meet a variety of business needs:

(i) Transaction processing systems

(ii) Management information systems

(iii) Decision support systems

(iv) Executive information systems

(v) Expert systems.

Three of the above categories of systems are discussed below:

(i) **Transaction Processing Systems:** These systems are aimed at expediting and improving the routine business activities that all organisations engage. Standard operating procedures, which facilitate handling of transactions, are often embedded in computer programs that control the entry of data, processing of details, search and presentation of data and information. Transaction processing systems if properly computerised provide speed and accuracy and can be programmed to follow routines without any variance.

(ii) **Management Information Systems (MIS):** Transaction processing systems are operations oriented. In contrast, MIS assist managers in decision making and problem solving. They use results produced by the transaction processing systems, but they may also use other information. In any organization, decisions must be made on many issues that recur regularly and require a certain amount of information. Because the decision making process is well understood, the manager can identify the information that will be needed for the purpose. In turn, the information systems can be developed so that reports are prepared regularly to support these recurring decisions.

(iii) **Decision Support Systems:** Not all decisions are of a recurring nature. Some occur only once or recur infrequently. Decision support systems (DSS) are aimed at assisting managers who are faced with unique (non-recurring) decision problems. In well structured situations, it is possible to identify information needs in advance, but in an unstructured environment, it becomes difficult to do so. As information is acquired, the manager may realize that additional information is required. In such cases, it is impossible to pre-design system report formats and contents. A DSS must, therefore, have greater flexibility than other information systems. Finally, we can say that DSS is of much more use when businesses are of an unstructured or semi-structured in nature. A decision support system is an integrated piece of software incorporating data base, model base and user interface. While the decision-support system can be of use at the tactical level, it is the strategic level that could make best use of it.

For details to above points, refer to study material, Chapter- 2 to 5.

(b) The benefits of successful Materials Requirement Planning (MRP) systems include:

(i) Significantly decreased inventory levels and corresponding decreases in inventory carrying costs.

(ii) Fewer stock shortage, which cause production interruptions and time-consuming schedule juggling by managers,

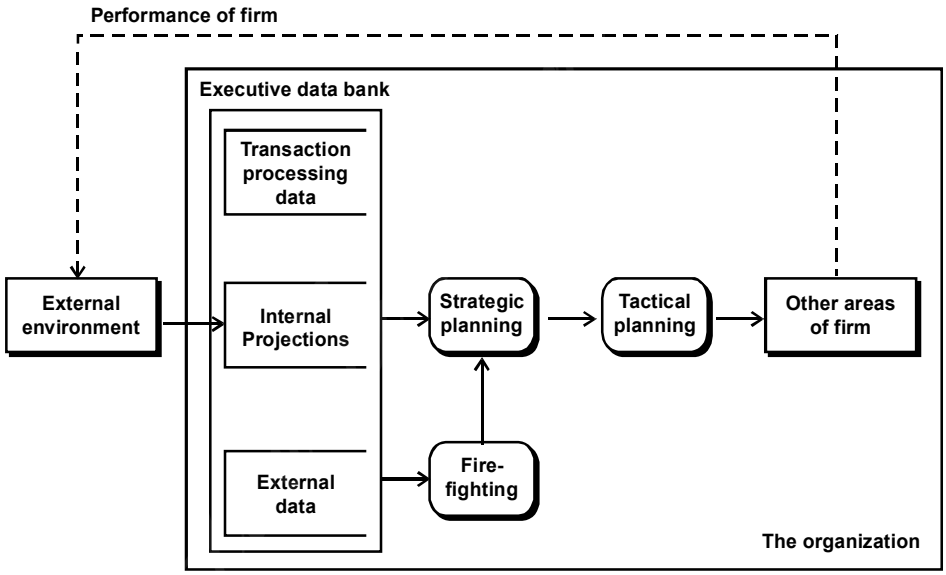
(iii) Increased effectiveness of production supervisors and less production chaos.

(iv) Better customer service - an increased ability to meet delivery schedules and to set delivery dates earlier and more reliably.

(v) Greater responsiveness to change. MRP gives manufacturing a better feel for the effects of economic swings and changes in product demand can be translated into schedule changes quickly.

(vi) Closer coordination of the marketing, engineering, and finance activities with the manufacturing activities.

5. (a) The data flow representation of the executive decision planning environment is given below:



(b) A practical set of principles to guide the design of measures and indicators to be included in an Executive Information System (EIS) are as follows:

(i) 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.

(ii) EIS measures must be based on a balanced view of the organization's objective. Data in the system should reflect the objectives of the organisation in the areas of productivity, resource management, and quality and customer service.

(iii) 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.

(iv) 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.

(v) 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.

(vi) EIS measures must evolve to meet the changing needs of the organization.

6. (a) The control techniques that are essential for the security of the client/server environment are as follows:

- Access to data and application is secured by disabling the floppy disk drive and USB drives etc.
- Diskless workstation prevents unauthorized access.
- Unauthorized users may be prevented from overriding login scripts and access by securing automatic boot or start-up 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 can be used to protect data from unauthorized access.
- Authentication systems can be provided to a client, so that they can enter into system, only by entering login name 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 those are required to perform their duties.

(b) The four categories of risks associated with client / server model are briefly discussed below:

(i) **Technological Risks:** The technological risk is quite simple. The first risk is – Will the new system work? But more important is the risk that in the long run the system may 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.

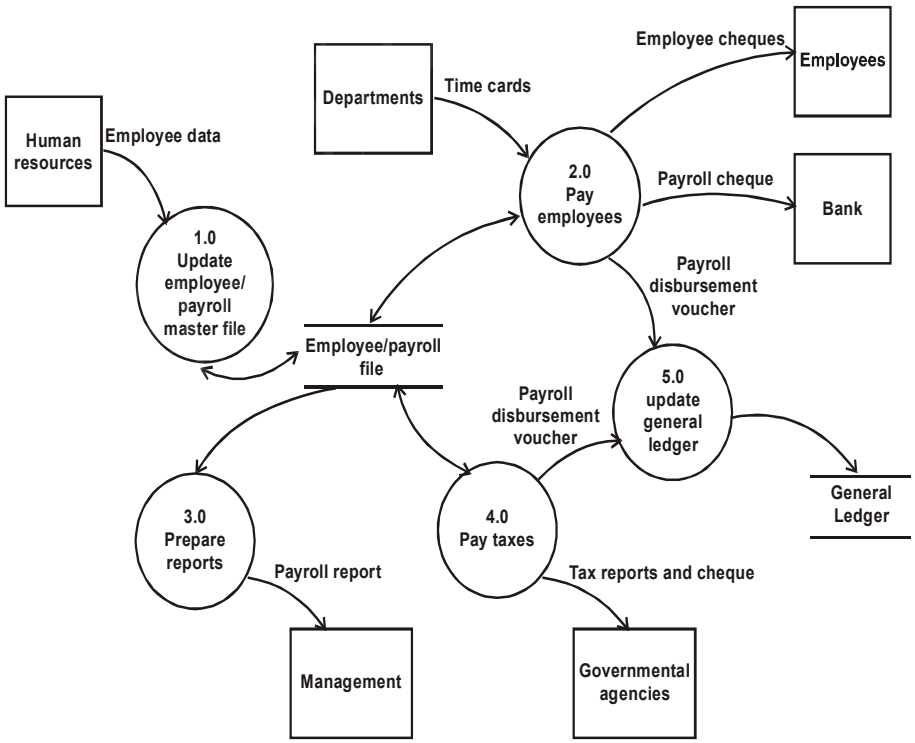
(ii) **Operational Risk:** These risks parallel the technological risks in both the short and long run. Respectively, they are – Will you achieve the performance you need from the new technology and will the software that you chose be able to grow or adapt to the changing needs of the business.

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

(iv) **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.

For details to above points, refer to study material, Chapter-6, Section 6.6

7. (a) The data flow diagram for the payroll processing system is given below:



(b) **Data Dictionary**: A data dictionary is a computer file that contains descriptive information about the data items in the files of a business information system. Thus, a data dictionary is a computer file about data. Each computer record of a data dictionary contains information about a single data item used in a business information system. This information may include:

(i) Codes describing the data item's length (in characters), data type (alphabetic, numeric, alphanumeric, etc.), and range (e.g., values from 1 to 99 for a department code)

(ii) The identity of the source document(s) used to create the data item.

(iii) The names of the computer files that store the data item.

(iv) The names of the computer programs that modify the data item.

(v) The identity of the computer programs or individuals permitted to access the data item for the purpose of file maintenance, upkeep, or inquiry.

(vi) The identity of the computer programs or individuals not permitted to access the data item.

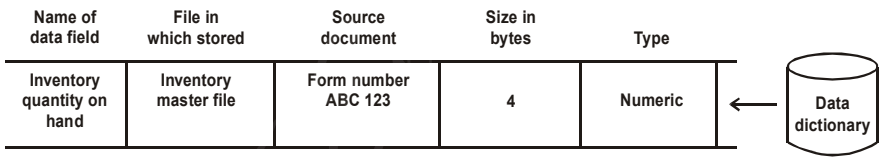


Figure: A sample record from a data dictionary.

Data dictionaries have a variety of uses. One is as a documentation aid to programmers and system analysts, who study, correct, or enhance either the database or the computer programs that access it. As suggested in points (v) and (vi) in the previous list, a data dictionary is also useful for file security – e.g., to prohibit certain employees from gaining access to sensitive payroll data.

Accountants and auditors can also make good use of a data dictionary. For example, a data dictionary can help establish an audit trail because it can identify the input sources of data items, the computer programs that modify particular data items, and the managerial reports on which the data items are output. When an accountant is participating in the design of a new system, a data dictionary can also be used to plan the flow of transaction data through the system.

Finally, a data dictionary can serve as an important aid when investigating or documenting internal control procedures. This is because the details about edit tests, methods of file security, and similar information can be stored in the dictionary.

8. **(a)** The manner in which data are physically arranged is referred to as format. This arrangement is called output format when referring to data output on a printed report or on a display screen. The different formats in which information can be presented are as follows:

(i) **Tabular format:** In general, end users are most accustomed to receiving information in a tabular form. Accountants and those who regularly review financial data rely exclusively on tabular information. Common examples of tabular reports are inventory control, accounts payable, general ledger, sales analysis and production scheduling reports. In general, the tabular format should be used when details dominate and few narrative comments or explanations are needed, details are presented in discrete categories, each category must be labeled and totals must be drawn or comparison made between components.

Certain information in a tabular format is more important and should be more visible than other information. This will vary by applications, but in general we can list down the items that should be included in tabular outputs:

(i) Exceptions to normal expectations.

(ii) Major categories or groups of activities or entities.

(iii) Summaries of major categories or activities.

(iv) Unique identification information.

(v) Time dependent entities.

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

(ii) **Graphic Format:** Graphic systems are available across a wide range of prices and capabilities and from personal computers up to mainframes. Management presentations have been enhanced by graphics and visuals for a long-time. Due to the availability of low cost but powerful computer software that uses data from existing data bases and produces high quality charts and diagrams, graphics outputs are becoming very popular. Graphics are used for several reasons. They are used to improve the effectiveness of output reporting for the targeted recipients, to manage information volume and to suit personal preferences.

Graphics are superior to tabular and narrative forms of information display for detecting trends in business performance. Comparisons are also easier through graphics than through tabular data. Graphic presentations also facilitate remembering large amounts of data throughout a series of reports.

In designing graphical output, the systems analyst must determine the purpose of the graph, the kind of data that need to be displayed, its audience and the effects on the audience of different kinds of graphical outputs. Graphic output also contains text, the design of which is an important aspect. Each graphic report, whether printed or displayed, should include a title and the date of preparation. For a series, page numbers should also be included. Labels can increase the accuracy with which people read data in bar graph form. However, placement of the label affects readability. Consistent spacing in all labels and using a common family of type styles maximize readability. All vertical and horizontal axes should be proportional. The use of all capital letters in long words, titles or foot notes impedes readability and thus should be avoided. Abbreviation should not be used.

Graphical output can be enormously useful to decision-makers if they are trained how to interpret it and when to use it.

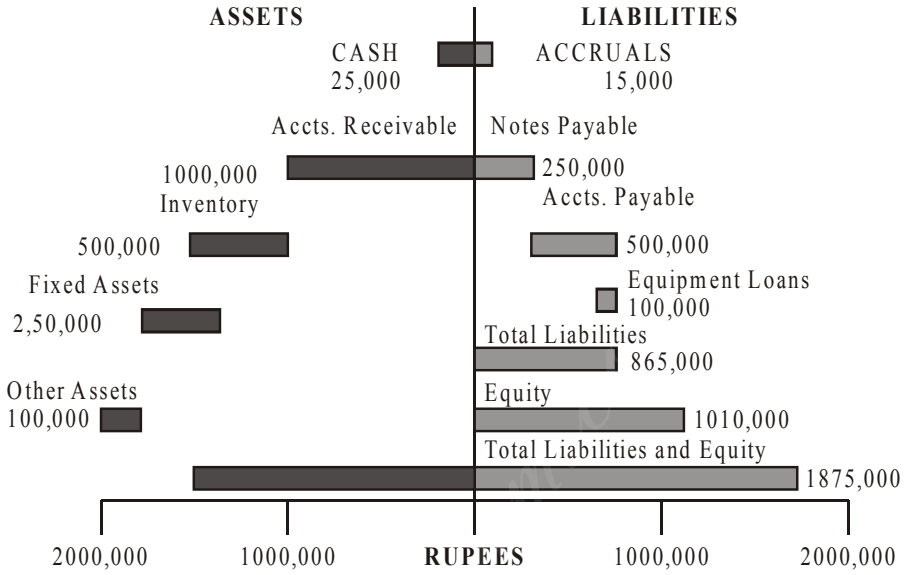


Figure : A sample graphic output

For details to above points, refer to study material, Chapter-8, Section 8.2.3.

(b) The basic output of the system design is a description of the task to be performed, complete with layouts and flowcharts. This is called the job specifications manual or system manual. The information included in the system manual contains:

(i) General description of the existing system.

(ii) Flow of the existing system.

(iii) Outputs of the existing system: The documents produced by existing system are listed and briefly described, including distribution of copies.

(iv) General description of the new system: Its purposes and functions and major differences from the existing system are stated together with a brief justification for the change.

(v) Flow of the new system: This shows the flow of the system from and to the computer operation and the flow within the computer department.

(vi) Output Layouts.

(vii) Output distribution: The distribution of the new output document is indicated and the number of copies, routing and purpose in each department shown. The output distribution is summarized to show what each department will receive as a part of the proposed system.

(viii) Input layouts: The inputs to the new system are described and complete layouts of the input documents and input disks or tapes provided.

(ix) Input responsibility: The source of each input document is indicated as also the user department responsible for each item on the input documents.

(x) Macro-logic-the overall logic of the internal flows will be briefly described by the systems analyst, wherever useful.

(xi) Files to be maintained: The specifications will contain a listing of the tape, disk or other permanent record files to be maintained, and the items of information to be included in each file. There must be complete layouts for intermediate or work file; these may be prepared later by the programmer.

(xii) List of programs: A list of the programs to be written shall be a part of the systems specifications.

(xiii) Timing estimates: A summary of approximate computer timing is provided by the systems analyst.

(xiv) Controls: This shall include type of controls, and the method in which it will be operated.

(xv) Audit trail: A separate section of the systems specifications shows the audit trail for all financial information. It indicates the methods with which errors and defalcation will be prevented or eliminated.

(xvi) Glossary of terms used.

9. (a) The following points may be considered while selecting a computer system:

- Today all computer systems available in the market have good hardware, competent software and roughly similar facilities. Due to rapid advances in computer technology, more recent computers are better in performance and the lower in cost. Hence as far as possible, the latest possible technology should be acquired in general.
- Commercial data processing involves mainly reading-in-data, printing data, storing and retrieving information from media. For commercial work computer performance is affected by the speed and capabilities of input/output and storage peripherals in contrast to scientific, engineering and operations problems which require good computational facilities, hence the efficiency of a computer system in handling such problems will depend on the main storage available. A comparison along these lines may be made.
- The software supplied by the manufacturer may make a significant difference if it contains a package of special applicability to the jobs envisaged. The selection of computer can also be made on software considerations. While all manufacturers supply general software packages for documentation and linear programming etc, a few manufacturers also offer packages specially designed for a particular industry such as Accounting applications in banking and insurance. Obviously, a manufacturer who has a package for users' special needs will enjoy a significant advantage.

- Modern computers are marketed as series of compatible, increasingly powerful and interchangeable peripherals. After some period, work expands beyond to fit in the existing computer needing higher capacity machine. Also, in case of breakdown, compatibility allows a wider range of machines to be used as back-up. Thus, the choice of a computer really becomes the choice of the model within the series, based on the long-range plan of expansion. But dependence on vendor/server is preferable to reprogramming which can be prohibitively expensive or time consuming. The selection of the computer configuration and a plan for its gradual expansion, as a properly considered model can save a great deal of money. The computer systems must be forward and backward compatible.
- Outside assistance in computer selection can be had from computer manufacturers, independent consultants specializing in computers, or management consulting firms. The distinction between vendor selection and machine selection is essentially a matter of business judgment. Once, however, the vendor is selected, he can be counted upon to provide useful guidance for machine also.

Point scoring Table for 'Ready to use' software:-

Software Evaluation Criteria	Possible points	Vendor A	Vendor B	Vendor C
Does the software's meet the mandatory specifications?	10	7	9	6
Will program modifications, if any, be minimal to meet company needs?	10	8	9	7
Does the software contain adequate controls?	10	9	9	8
Is the performance (speed, accuracy, reliability etc.) adequate?	10	7	9	6
Are other users satisfied with the software?	8	6	7	5
Is the software user-friendly?	10	7	8	6
Can the software be demonstrated and test-driven?	9	8	8	7
Does the software have an adequate warranty?	8	6	7	6
Is the software flexible and easily maintained?	8	5	7	6
Is online inquiry of files and	10	8	9	7

records possible?				
Will the vendor keep the software up to date?	10	8	8	7
Total	**123**	**94**	**106**	**85**

It may be noted that the data shown above are indicative only.

For details to above points, refer to study material, Chapter 9, Section 9.1.

(b) The various steps involved in system testing are as follows:

- Preparation of realistic test data in accordance with the system test plan,
- Processing the test data using the new equipment,
- Thorough checking of the results of all system tests, and
- Reviewing the results with future users, operators and support personnel.

One of the most effective ways to perform system-level testing is to perform parallel operations with the existing system. Parallel operations consist of feeding both systems the same input data and comparing data files and output results. Despite the fact that the individual programs were tested, related conditions and combinations of conditions that were not envisioned are likely to occur. Last minute changes to computer programs are necessary to accommodate these new conditions.

During parallel operations, the mistakes detected are often not those of the new system, but of the old. These differences should be reconciled as far as it is feasible economically. Those responsible for comparing the two systems should clearly establish that the remaining deficiencies are caused by the old system. A poor checking job at this point can result in complaints later from customers, top management, salespersons, and others. Again, it is the responsibility of the system developers and analysts to satisfy themselves that adequate time for dual operations has been undertaken for each functional area changed.

For details to above points, refer to study material, Chapter-9, Section 9.7

10. (a) There are five strategies for converting from the old system to the new system. They are as follows:

(i) *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.

(ii) *Parallel conversion*: This refers to running the old system and the new system at the same time, in parallel. This is the most frequently used conversion approach, but its popularity may be in decline because it works best when a computerised system replaces a manual one. Both systems are run simultaneously for a specified period of time and the reliability of results is examined. When the same results are gained over time, the new system is put into use and the old one is stopped. The advantage of running both systems in parallel includes the possibility of checking new data against old data in order to catch any errors in processing in the new system. Parallel processing also offers a feeling of security to users, who are not forced to make an abrupt change to the new system.

(iii) *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.

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

(v) *Distributed conversion*: This refers to a situation in which many installations of the same system are contemplated, such as in banking or in franchises such as restaurants or clothing stores. One entire conversion is done (with any of the four approaches considered already) at one site. When that conversion is successfully completed, other conversions are done for other sites. An advantage of distributed conversion is that problems can be detected (and contained) rather than inflicting them, in succession, on all sites.

For details to above points, refer to study material, Chapter-10, Section 10.3.

(b) Most information systems require at least some modification after development. The need for modification arises from a failure to anticipate all requirements during system design and/or from changing organisational requirements. The changing organisational requirements continue to impact most information systems as long as they are in operation. Consequently periodic systems maintenance is required for

most of the information systems. Systems maintenance involves adding new data elements, modifying reports, adding new reports, changing calculations, etc.

Maintenance can be categorised in the following two ways:

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

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

11. (a) The various outputs of the inventory control system include the following:

(i) Inventory transactions listing for control purpose.
(ii) Inventory ledger
(iii) Customer's report
(iv) Back-orders file report
(v) Excess-stock
(vi) Under-stock
(vii) Slow-moving
(viii) ABC class items

Exception reports

(ix) Items-to-do ordered file.

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

(b) 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 (if any), the number of shares held, and the identification of the certificates through which these shares are held.

When a person purchases shares from a share holder, a share transfer form along with the certificates is sent by the buyer to the company for incorporating the transfer. The system records a change in ownership for the shares from the seller to the buyer. Periodically, the company declares a dividend. Dividend warrants (cheques) need to be mailed on a particular day to the various shareholders who hold shares. Calculation of income tax to be deducted at source is also done before the printing and mailing dividend warrants.

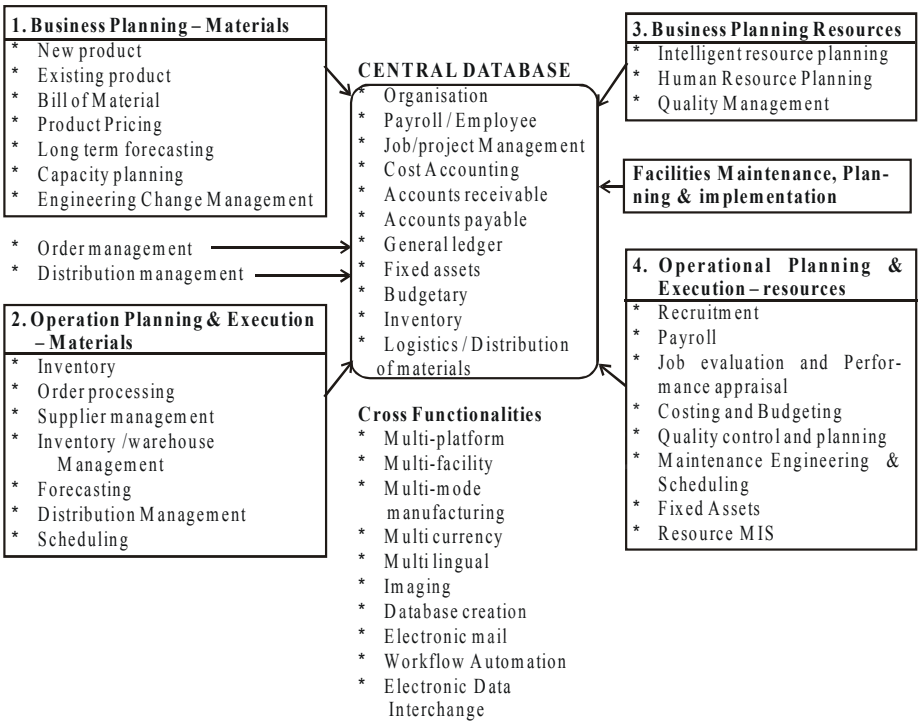
Other facilities usually provided in share accounting system are:

- Bank mandate facility, where the shareholder's dividend warrant is sent to a bank account at the 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.
- Mailing annual reports and invitations to various meetings.

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

In simple words, Enterprise resource planning promises one database, one application, and one user interface for the entire enterprise, where once disparate systems ruled manufacturing, distribution, finance and sales. Taking information from every function it is a tool that assists employees and managers' plan, monitor and control the entire business. A modern ERP system enhances a manufacturer ability to accurately schedule production, fully utilize capacity, reduce inventory, and meet promised shipping dates.

A general model of ERP is shown below.



13. (a) The list of some of the entities forming a data model in business modelling is given in a table below:

Entity	Description
External data	Entities outside the firm that interact with it, such as customers, suppliers, competitors and distributors. Also includes predictive data regarding economy and future events in external environment.
Internal data	Data generated from the firm's transaction processing system, internal forecasts or parameters monitored.
Funding data	Includes information on specific sources of funds as well as availability terms and conditions etc.
Marketing research data	Mainly consumer related data that can be used to support marketing decisions and result of surveys.
Production data	Shop floor data on production processes including standards and actual of time and material resources concerned.
Inventory data	Includes inventories of raw materials goods in progress and finished goods.
Personnel data	Mostly includes profiles of employees, their skill levels, experience and past performance on various assignments.

Sales forecast	Product-wise and period-wise forecast for various products sold by the company.
Payroll data	Data about salaries, tax deductions, statutory forms and other deductions
General ledger	Integrated transaction data from pay roll and account receivable. It is the basis for budgeting and planning data.

(b) Some of the major reasons for ERP adoption by the company are as follows:

- ERP provides complete integration of systems not only across departments but also across companies under the same management.
- ERP facilitates company-wide Integrated Information System covering all functional areas like manufacturing, selling and distribution, payables, receivables, inventory, accounts, human resources, purchases etc.
- ERP eliminates most business problems like material shortages, productivity enhancements, customer service, cash management, inventory problems, quality problems, prompt delivery etc.
- Has end to end Supply Chain Management to optimize the overall Demand and Supply Data.
- ERP provides multi-platform, multi-facility, multi-mode manufacturing, multi-currency, multi-lingual facilities.
- It supports strategic and business planning activities, operational planning and execution activities, creation of Materials and Resources. All these functions are effectively integrated for flow and update of information immediately upon entry of any information.
- ERP performs core activities and increases customer service, thereby augmenting the corporate image.
- ERP bridges the information gap across organisations.
- ERP is the solution for better project management.
- ERP allows automatic introduction of the latest technologies like Electronic Fund Transfer (EFT), Electronic Data Interchange (EDI), Internet, Intranet, Video conferencing, E-Commerce etc.
- ERP provides intelligent business tools like decision support system, Executive information system, Data mining and easy working systems to enable better decisions.

For details to above points, refer to study material, Chapter-12, Section 12.1.

14. The various threats to operating system integrity are:

(i) *Accidental threats*: These types of threats include hardware failures that cause the operating system to crash. Operating system failures are also caused by errors in user application program that the operating system cannot interpret. Accidental

system failures may cause whole segments of memory to be "dumped" to disks and printers, resulting in the unintentional disclosure of confidential information.

(ii) *Intentional threats*: These types of 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 organisation 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.

For details to above points, refer to study material, Chapter-13, Section 13.2.2

15. The risk to computer system can be controlled through system design, installation of security measures and regular security audit. However, some residual risks always exist that cannot be covered. One way of handling this residual risk is to transfer it contractually to a third party by way of insurance of the computer installation.

If a decision is made to purchase insurance cover, management must be careful to ensure that they consider all major potential losses; the replacement cost of purchased or leased hardware must be covered, special construction relating to raised floors and air conditioning must be covered etc. The types of insurance policies that might be obtained are:

- Data processing policy
- Valuable papers and records policy
- Business interruption insurance
- Extra expense insurance.
- Errors and omissions insurance.

16. Denial of service attacks can severely hamper an organisation's ability to use the Internet to conduct commerce. Although this activity cannot currently be prevented, there are two actions that management and accountants can take to limit the exposure. First, the firewalls at the source site can be programmed to block messages with non-internal addresses. This would prevent attackers from hiding their locations from the targeted site and would assure the organisation's management that no undetected attacks could be launched from its site. This strategy will not, however, prevent attacks from areas of the Internet that do screen outgoing transmissions.

Second, security software is available for the targeted sites that scan for half open connections. The software looks for SYN packets that have not been followed by an ACK packet. The clogged ports can then be restored to allow legitimate connections to be made.

For details to above points, refer to study material, Chapter-13, Section 13.8.1.

17. The three levels of input validation controls are:

(i) **Data Coding controls:** Coding controls are checks on the integrity of data codes used in processing. A customer's account number, an inventory item number, and a chart of accounts number are all examples of data codes. Three types of errors can corrupt a data code and cause processing errors: transcription, single transposition and multiple transposition. Check digit can be used to ensure integrity of the code in subsequent processing.

(ii) **Validation controls:** Input validation controls are intended to detect errors in transaction data before the data are processed. Validation procedures are most effective when they are performed as close to the source of the transaction as possible. However, depending on the type of CBIS in use, input validation may occur at various points in the system. There are three levels of validation controls: field interrogation, transaction interrogation and file interrogation.

(iii) **Input Error Correction:** When errors are detected in a batch they must be corrected and the records resubmitted for reprocessing. This must be a controlled process to ensure that errors are dealt with completely and correctly. There are three common error handling techniques: immediate correction; create an error file, and reject the entire batch.

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

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

(i) **Limit check**: This is a basic test for data processing accuracy and may be applied to both the input and output data. The field is checked by the program against predefined limits to ensure that no input/output error has occurred or at least no input error exceeding certain pre–established limits has occurred.

(ii) **Picture check**: Under this check, only certain characters are allowed in a data field. The computer can test the field to determine that no invalid characters are used.

(iii) **Valid code check**: If there are a limited number of valid codes, the code being read may be checked against pre–determined transaction codes, or table to ensure that it is one of the valid codes.

(iv) **Check digit**: It is an extra digit that is computed from the code itself and placed alongside it for subsequent checking. There are a number of check digit schemes. 11-Module check digit scheme has been empirically established as the best to detect transposition errors.

(v) **Arithmetic check**: Arithmetic check is performed in different ways to validate the results of other computations or the value of selected data field.

(vi) **Valid combinations of fields**: In addition to each of the individual fields being tested, combination of fields may be tested for validity.

(vii) **Cross check**: It may be employed to verify fields appearing in different files to see that the results tally.

(viii) **Valid field size, sign and composition**: If the code number should be specified number of digits in length, the computer may be programmed to test that the field size is as specified. If the sign of the field must always be positive or always negative, a test may be made to determine that the field does indeed contain a proper composition of characters.

The various types of transaction checks are given below:

(i) Sequence checks are exercised to detect any missing transactions, off–serially numbered vouchers.

(ii) Format completeness checks are used to check the presence and position of all the fields in a transaction.

(iii) Redundant data checks are employed to check the validity of codes with reference to the description.

(iv) Checks may be incorporated to ensure that transactions pertain to the correct period.

(v) Combination checks may be exercised on various fields of a file.

(vi) Passwords may be issued to check entry of data by unauthorised persons in on–line systems.

(vii) Probability checks are used to avoid unnecessary rejection of data as data can, on occasions, exceed normal values in a range due to purely random causes.

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

19. (a) The various sources from where the information can be recovered to investigate computer frauds are as follows:

- Free space: It refers to areas of a file system not currently allocated for data storage. These areas may have been used before and may contain deleted data, which has not yet been overwritten.
- Lost chains: It refers to areas of the disk allocated for data storage but currently without a name or disconnected from the file system.
- Slack space: It refers to disk space allocated to files in allocation blocks normally of several hundred to several thousand bytes in size. Files rarely occupy a complete number of allocation blocks so some of the last allocation

block will be unused. This area may contain data, which has not been overwritten.

- Deleted files: Files that have been "undeleted" by the processing software and made available for interrogation.
- The contents of the Windows SWAP file: This is a disk cache created by Windows each time it is run. It is a storage area in which all kinds of data may be kept. The file may be large and is hidden from the user. It is seldom deleted and can contain entire documents, memoranda and database information. It can thus be extremely valuable to an investigator.
- Internet cache files or temporary Internet files: When the Internet is accessed through Windows, copies of the web pages looked at by the user are copied to the user's computer. These copies are stored in a folder called Temporary Internet files. They can be of great interest to the investigator as it might provide a route map of Internet access.

(b) 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 findings are 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.

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.

20. Some of the important terms as defined in the Information Technology Act 2008 (Amended) are:

(a) "*asymmetric crypto system*" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;

(b) "*electronic form*" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

(c) "*electronic record*" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

(d) "Electronic signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature

(e) "Electronic Signature Certificate" means an Electronic Signature Certificate issued under section 35 and includes Digital Signature Certificate"

For details to IT Act (Amended 2008), refer to the link http://www.icai.org/post.html?post_id=1056

21. The chapter VIII of the Information Technology Act 2008 (Amended) containing sections 35 to 39 lay down procedures relating to digital signature certification. The Certifying Authority may suspend such certificate if it is of the opinion that such a step needs to be taken in public interest.

Subject to the provisions of sub-section (2), the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate -

(a) On receipt of a request to that effect from -

(i) The subscriber listed in the Digital Signature Certificate; or

(ii) Any person duly authorized to act on behalf of that subscriber;

(b) If it is of opinion that the Digital Signature Certificate should be suspended in public interest

A Digital Signature Certificate shall not be suspended for a period exceeding fifteen days unless the subscriber has been given an opportunity of being heard in the matter.

On suspension of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

Section 38 provides for the revocation of Digital Signature Certificate under certain circumstances. Such revocation shall not be done unless the subscriber has been given an opportunity of being heard in the matter. Upon revocation or suspension, the Certifying Authority shall publish the notice of suspension or revocation of a Digital Signature Certificate.

For details to IT Act (Amended 2008), refer to the link http://www.icai.org/post.html?post_id=1056

22. (a) The purpose of an IS audit is to review and evaluate the internal controls that protect the system. When performing an IS audit, Auditors should ascertain that the following objectives are met:

(i) Security provisions protect computer equipment, programs, communications, and data from unauthorized access, modification, or destruction.

(ii) Program development and acquisition is performed in accordance with management's general and specific authorization.

(iii) Program modifications have the authorization and approval of management.

(iv) Processing of transactions, files, reports, and other computer records is accurate and complete.

(v) Source data that is inaccurate or improperly authorized is identified and handled according to prescribed managerial policies.

(vi) Computer data files are accurate, complete, and confidential.

(b) Test Data Processing: One way to test a program is to process a hypothetical series of valid and invalid transactions. The program should process all of the valid transactions correctly and identify and reject all of the invalid ones. All logic paths should be checked for proper functioning by one or more of the test transactions. Examples of invalid data include records with missing data, fields containing unreasonably large amounts, invalid account numbers or processing codes, non-numeric data in numeric fields, and records out of sequence.

Several resources are available when preparing test data. For example:

- A listing of actual transactions.
- The test transactions that the programmer used to test the program.
- A test data generator program, which automatically prepares test data based on program specifications.

In a batch processing system, the company's program and a copy of relevant files are used to process the test data. The results are compared with the pre-determined correct output; discrepancies indicate processing errors or control deficiencies that should be thoroughly investigated.

23. (a) **Security Objective:** The objective of information security is "the protection of the interests of those relying on information, and the information systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality, and integrity".

For any organization, the security objective is met when:

- information systems are available and usable when required (availability);
- data and information are disclosed only to those who have a right to know it (confidentiality); and
- data and information are protected against unauthorized modification (integrity). The relative priority and significance of availability, confidentiality, and integrity vary according to the data within the information system and the business context in which it is used.

(b) The various ways to protect computer held information can be classified into two types: Preventative and Restorative.

(i) *Preventative Information Protection*: This type of protection is based on use of security controls. Information security controls are generally grouped into three types of control: Physical, Logical, and Administrative. Organizations require all three types of controls. The organization's Information Security Policy through the associated Information Security Standards documentation mandates use of these controls. Here are some examples of each type of control:

- Physical: Doors, Locks, Guards, Floppy Disk Access Locks, Cables locking systems to desks/walls, CCTV, Paper Shredders, Fire Suppression Systems
- Logical (Technical): Passwords, File Permissions, Access Control Lists, Account Privileges, Power Protection Systems
- Administrative: Security Awareness, and User Account Revocation Policy.

(ii) *Restorative Information Protection*: Security events that damage information will happen. If an organization cannot recover or recreate critical information in an acceptable time period, the organization will suffer and possibly have to go out of business. Planning and operating an effective and timely information backup and recovery program is vital to an operation. Information backup does not simply involve backing up "just the valuable information," but it frequently also means backing up the system as well, since the information may need services that the system provides to make the information usable.

The key requirement of any restorative information protection plan is that the information can be recovered. This is frequently an issue that many organizations fail to properly address. There is a common belief that if the backup program claimed it wrote the information to the backup media, it can be

recovered from the backup media. However, there are many variables that can prove that belief wrong.

Here are a few questions any restorative information protection program must address:

- Has the recovery process been tested recently?
- How long did it take?
- How much productivity was lost?
- Did everything go according to plan?
- How much extra time was needed to input the data changes since the last backup?

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

24. (a) The table given below lists a number of different types of CASE tools and gives specific examples of each tool.

Tool type	**Example**
Management tools	PERT tools, estimation tools
Editing tools	Text editors, diagram editors, word processors
Configuration management tools	Version management system, change management system
Prototyping tools	High level language tools, user interface generators
Method support tools	Design editors, data dictionaries, code generators
Language processing tools	Compilers, interpreters
Program analysis tools	Cross reference generators, static analyzers, dynamic analyzers
Testing tools	Test data generators, file compactors
Debugging tools	Interactive debugging system
Documentation tools	Page layout program, image editors
Reengineering tools	Cross reference systems, program restructuring systems

(b) Data integration is the process of exchange of data by CASE tools. The result from one tool can be passed as input to another tool. There are a number of different levels of data integration:

(a) *Shared files*: All tools recognize a single file format. The most general purpose

shareable file format is where files are made of lines of characters.

(b) *Shared data structures*: The tools make use of shared data structures which usually include program or design language information.

(c) Shared repository: The tools are integrated around an object management system which includes a public share data model describing the data entities and relationships which can be manipulated by the tools.

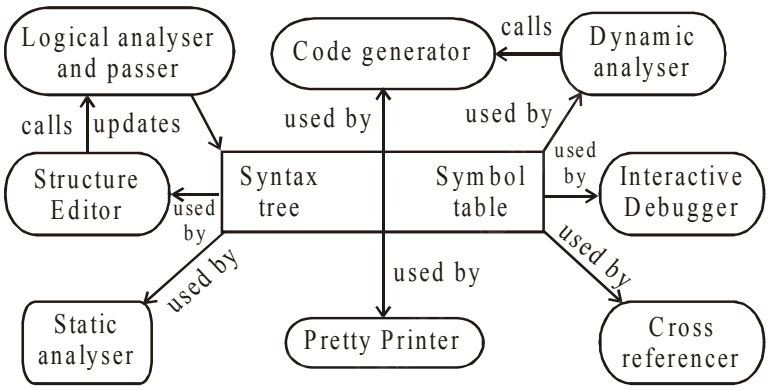
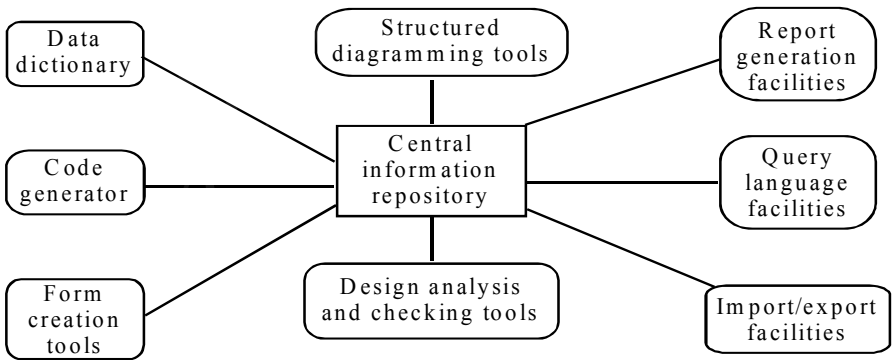


Figure: Integration through shared data structure

25. 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 the figure below:



The components of this model are:

(i) *Diagram editors* to create data flow diagrams, structured charts, entity relationship diagram and so on.

(ii) *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.

(iii) *Repository query languages* which allow the designer to find the designs and associate design information in the repository.

(iv) *A* data dictionary which maintains precise and unambiguous information about all data elements used in a system design.

(v) *Report definition and generation* tools which take information from the central store and automatically generate system documentation.

(vi) *Forms definition tools* which allow screen and document formats to be specified.

(vii) *Import-export facilities* which allow the interchange of information from the central repository with other development tools.

(viii) *Code generators* which generate code or code skeletons automatically from the design captured in the central store.