

PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

Question No 1 is compulsory.

*Attempt any **five** questions from the remaining **six** questions.*

Question 1

- (a) *What are the various stages involved in the top-down approach of System Development Process?* (5 Marks)
- (b) *What are the benefits of Material Requirement Planning?* (5 Marks)
- (c) *State how computer fraud differs from conventional fraud.* (5 Marks)
- (d) *Give any five objectives of Information Technology Act, 2008.* (5 Marks)

Answer

- (a) Various stages involved in the top-down approach of System Development Process are as follows:
- (i) Analyze the objectives and goals of the organization to determine where it is going and what management wants to accomplish. The analysis may be started in terms of profits, growth, expansion of product line or services, diversification, increased market share and so on. It is also determined what resources are available in terms of capital, equipments and raw material.
 - (ii) Identify the functions of the organization (e.g. marketing, production, research and development) and explain how they support the entire organization.
 - (iii) Based on the functions identified, ascertain the major activities, decisions and functions of the managers at various levels of hierarchy. It should also be analyzed what decisions are made as well as what decisions need to be made and when they should be made.
 - (iv) With activities and decisions identified, identify models that guide managerial decision processes and find out the information requirements for activities and decisions. An insight should be provided into what information is needed when it is needed and what form is most useful. These factors provide many of the design specifications for the application systems.
 - (v) Prepare specific information processing programs in detail and modules within these programmes. Also identify files and data base for the application.
- (b) The benefits of a successful MRP system include:
- Significantly decreased inventory levels and corresponding decrease in inventory carrying costs.
 - Fewer stock shortages, which cause production interruptions and time consuming schedule juggling by managers.
 - Increased effectiveness of production supervisors and less production chaos.

FINAL (OLD) EXAMINATION : NOVEMBER, 2010

- Better customer service- an increased ability to meet .delivery schedules and to set delivery dates earlier and more reliably.
 - 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.
 - Closer coordination of the marketing, engineering, and finance activities with the manufacturing activities.
- (c)** Computer fraud differs from conventional fraud in a number of important respects, which are given as follows:
1. It is easily hidden and hard to detect. Unlike conventional fraud, there may be no easily recognizable audit trail and the fraud is likely to be hidden in enormous volumes of data.
 2. Evidence of computer crimes may be not only hard to find, but also difficult to present to a court in a way which is effective or legally admissible. Anyone who has prosecuted or defended computer crime cases will be aware of the problems of obtaining evidence in the first place, ensuring that it complies with the relevant statutes and trying to explain it to an inexperienced judge or jury.
 3. It is easily committed in ways that may not be obvious:
 - it involves the manipulation of "invisible" data;
 - a few key strokes are all that may be needed;
 - a business's computer can be remotely accessed, both by employees and outsiders; and
 - huge amount of data can be transported on a single CD, which can be written to in a matter of seconds. .
 4. Lack of knowledge about how computer works and how systems can be protected against fraudsters to take advantage.
 5. The damage caused by interference with computer systems can be out of all proportion to the effort required to cause the damage.
- (d)** The objectives of the Information Technology Act are:
- (i) to grant legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication;
 - (ii) to give legal recognition to Digital signature for authentication of any information or matter, which requires authentication under any law;
 - (iii) to facilitate electronic filing of documents with Government departments;
 - (iv) to facilitate electronic storage of data;

PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

- (v) to facilitate and give legal sanction to electronic fund transfers between banks and financial institutions;
- (vi) to give legal recognition for keeping books of account by Bankers in electronic form; and
- (vii) to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934.

Question 2

- (a) *Discuss important fact-finding techniques that are used by the system analysis for determining the user requirements, during the system development process. (4 Marks)*
- (b) *As a head of an IS audit team what are the techniques you would expect your audit team to adopt in processing controls to preserve audit trails? (6 Marks)*
- (c) *A company is using client/server technique and believes that it is 100% risk free. As an IS auditor, would you endorse the view? Give four points to justify your answer.(6 Marks)*

Answer

- (a) The following fact finding techniques are used by the system analysts for determining the user requirements:
 - (a) **Documents** - Documents means manuals, input forms, output forms, diagrams of how the current system works, organization charts showing hierarchy of users and managers responsibilities, job descriptions for the people who work with the current systems procedure manuals, program codes etc. Documents are a very good source of information about user needs and the current system. They are easy to collect, convey a lot of information and provide relatively objective data. The analyst should ensure that the document, which s/he is collecting are current, accurate and contain up-to-date information.
 - (b) **Questionnaires** - Users and managers are asked to complete questionnaires about the information system when the traditional system development approach is chosen. The main strength of questionnaires is that a large amount of data can be collected through a variety of users quickly. If the questionnaire is skillfully drafted, responses can be analyzed rapidly with the help of a computer.
 - (c) **Interviews** - Users and managers may also be interviewed to extract information in depth. The data gathered through interviews often provides systems developer with a complete picture of the problems and opportunities. Interviews also give analyst the opportunity to note user reaction first - hand and to probe for further information
 - (d) **Observations** - In prototyping approach, observation plays central role in requirement analysis. Only by observing how users react to prototypes of a new system, the system can be successfully developed. In traditional approach, it is not always mandatory. The analyst should visit the user site to watch how the work was taking place. The value of observational visits by analysts can be great. A surprise

FINAL (OLD) EXAMINATION : NOVEMBER, 2010

visit often helps the analyst in getting a clear picture of the user's environment and to determine why a request for a new system was submitted.

- (b) The following are the examples of techniques to adopt in processing controls to preserve audit trails:

1. Transaction Logs

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

2. Transaction Listings

- The system should produce a transaction listing of successful transactions. These listings should go to appropriate users to facilitate reconciliation with input.

3. Log of Automatic Transactions

- Some transactions are triggered internally by the system. For example, when inventory drops below a preset reorder point, the system automatically processes a purchase order.
- To maintain an audit trail of these activities, all internally generated transactions must be placed in a transaction log.

4. Listing of Automated Transactions

- To maintain control over automatic transactions processed by the system, the responsible end user should receive a detailed listing of all internally generated transactions.

5. Unique Transaction Identifiers

- Each transaction processed by the system must be uniquely identified with a transaction number.

PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

- This helps to trace a particular transaction through a database of thousands or even millions of records.
- In systems that use physical source documents, the unique number printed on the document can be transcribed during data input and used for this purpose.
- In real - time systems, which do not use source documents, each transaction should be assigned a unique number by the system.

6. Error Listing

- A listing of all error records should go to the appropriate user to support error correction and resubmissions.

(c) No, it is not 100% risk free, though the benefits from Client/Server are truly praiseworthy, but there are also some risks and drawbacks in certain areas, which can be categorized as follows:

1. Technological Risks

- This 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. Then the next question becomes: how soon it will become obsolete.

2. 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.

3. 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 and the new client server architecture development.
- In the long run, the concern centers around the support costs of the new system.

4. 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 question is definitely not if the system is difficult to use or is plagued with problems.
- The long run question concerns costs.

FINAL (OLD) EXAMINATION : NOVEMBER, 2010

Question 3

- (a) *What is an Executive Information System? Explain its purposes.* (6 Marks)
- (b) *Mention the components of an Accounting Information System.* (4 Marks)
- (c) *Give some common types of field interrogation, involving programmed procedures that examine the characters of the data in the field.* (6 Marks)

Answer

(a) Executive Information System (EIS):

EIS is a tool that provides direct online access to relevant information in a useful and navigable format. Relevant information is timely, accurate, and actionable information about aspects of a business that are of particular interest to the senior manager. The useful and navigable format of the system means that it is specifically designed to be used by the individuals with limited time, limited keyboarding skills and little direct experience with computers.

An EIS is quite easy to navigate so that managers can identify broad strategic issues, and then explore the information to find the root causes of those issues.

Purpose of EIS:

1. The primary purpose of an EIS is to support managerial learning about an organization, its work process and its interaction with the external environment.
2. 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. In addition, 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.
3. 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 look upon 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.

PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

(b) The components of an Accounting Information System can be divided into four separate areas:

1. The general ledger systems, which include the general ledger, budgeting, and responsibility/profitability reporting.
2. The cash receipts/disbursements systems, which include the accounts payable, payroll and accounts receivable systems.
3. The production management system, which include the material inventory control, work-in-process control, cost estimation, and production scheduling systems.
4. The marketing systems, which include finished goods inventory control, order processing, and marketing analysis system.

(c) Field interrogation involves procedures that examine the characters of the data in the field. The following are some common types of the same:

1. Limit Checks

The field is checked by the program to ensure that its value lies within certain predefined limits (in the program). This applies to both input and output fields considered to be important. Several examples follow:

- Hours worked by an employee in a week cannot exceed, say 60. The program would verify this for each employee's clock card and where this limit is exceeded; an error message would either be printed or displayed. Thus, this is a safeguard against both inadvertent errors and fraud.
- Limit on weekly earnings of an employee.
- The highest vendor number is 3429. If the program encounters the vendor No. 4329, an error message would be printed.
- All customers with code 2, cannot purchase in excess of Rs. 20,000.
- No pay when there is sick leave.
- Physical balance can never go below zero. Likewise, wages, forecasts cannot go negative.
- Lowest and highest prices of stock items to ascertain that the price on each transaction is not beyond these.

2. Picture Checks

These check against entry into processing of incorrect characters. Example: All department numbers may be made up of numerics. An incorrect deptt. No. 4D3 would thus be filtered.

FINAL (OLD) EXAMINATION : NOVEMBER, 2010

3. Valid Code Checks

Checks are made against predetermined transactions codes, tables or other data to ensure that input data are valid. The predetermined codes/tables may either be embedded in the programs or stored in (direct access) files.

Example (i): In an inventory updation application, the following may be comprehensive list of transaction codes:

- I = Issue
- R = Receipts
- C = Allocations against customer orders
- A = Amendments
- D = Deletion
- N = Addition of new records
- S = Stock taking adjustments.
- Any other code (misc. punching for example) would be brought out in the error message.

Example (ii): Every time a payment is made to a vendor, the number of the vendor must match a number in the table of valid vendors.

Example (iii): A code 19 is assigned to the preventive maintenance. If one or several time card codes from preventive maintenance do not agree with this code, an error would be displayed.

Example (iv): In the codes table for the chart of accounts the current assets may be designated from 100 to 199, where cash is 100. If cash receipts are being processed all cash credits or debits must contain the code 100.

4. Check Digit

A check digit is a control digit (s), added to the code when it is originally assigned and allows the integrity of the code to be established during subsequent processing.

5. Arithmetic Checks

Arithmetic checks are performed in different ways to validate the result of other computations of the values of selected data fields.

- *Example (i) :* In payroll processing, it is usual to accumulate gross pay, deduction and net pay. At each employee's record whenever those totals are accumulated, the gross pay must equal net pay + deductions.
- *Example (ii) :* If x is to be divided by y not only this is done but also for verification, the quotient is multiplied by y to verify the result.

PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

6. Cross Checks

These may be employed to verify fields appearing in different files to check that the results tally. For example, the quantity received, quantity invoiced by the supplier and quantity ordered may be compared. Incidentally, it may also be necessary to affect a check on the units of quantity. Fraud is possible if the unit is *gm* on the transaction whereas the standard unit in the master file is *kg*.

Question 4

- (a) Explain any six limitations of Management Information System. (6 Marks)
- (b) What is the significance of system evaluation? How is it performed? (6 Marks)
- (c) Briefly describe the two general types of firewalls. (4 Marks)

Answer

- (a) The main limitations of MIS are given as follows:
 - (i) The quality of the outputs of MIS is basically governed by the quantity of input and processes.
 - (ii) MIS cannot replace managerial judgement in making decisions in different functional areas. It is only an important tool for decision making and problem solving.
 - (iii) MIS may not have requisite flexibility to quickly update itself with the changing needs of time, especially in fast changing and complex environment.
 - (iv) MIS cannot provide tailor-made information packages suitable for the purpose of every type of decision made by executives.
 - (v) MIS ignores non-quantitative factors, like morale and attitude of the members of the organization, which have an important bearing on the decision making process of executives.
 - (vi) MIS is less useful for making non-programmed decisions.
 - (vii) The effectiveness of MIS is reduced in organizations where the culture of hoarding information and not sharing with others holds/exists.
 - (viii) MIS effectiveness decreases due to frequent changes in top management, organizational structure and operational team.
- (b) The final step of the systems implementation is System evaluation. Evaluation provides the feedback necessary to assess the value of information and the performance of personnel and technology included in the newly designed system. This feedback serves two functions:
 - 1. It provides information as to what adjustments to the information system may be necessary.

FINAL (OLD) EXAMINATION : NOVEMBER, 2010

2. It provides information as to what adjustments should be made in approaching future information systems development projects.

There are two basic dimensions of information systems that should be evaluated. The first dimension is concerned with whether the newly developed system is operating properly. The other dimension is concerned with whether the user is satisfied with the information system with regard to the reports supplied by it.

Development evaluation: Evaluation of the development process is primarily concerned with whether the system was developed on schedule and within budget. This is a rather straightforward evaluation. However, it requires schedules and budgets to be established in advance and that records of actual performance and cost be maintained.

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:

1. Are all transactions processed on time?
2. Are all values computed accurately?
3. Is the system easy to work with and understand?
4. Is terminal response time within acceptable limits?
5. Are reports processed on time?
6. Is there adequate storage capacity for data?

Information evaluation: An information system should also be evaluated in terms of information it provides. This aspect of system evaluation is difficult and it cannot be conducted in a quantitative manner, as it is the case with development and operation evaluations. The objective of an information system is to provide information to support the organizational decision system. Therefore, the extent to which information provided by the system is supportive to decision making is the area of concern in evaluating the system. However, it is practically impossible to directly evaluate an information system's support for decision making in an organization. It must be measured indirectly.

- (c) The two general types of firewalls are described below:

Network-level firewalls – These provide low cost and low security access control. This type of firewall consists of screening router that examines the source and destination addresses that are attached to incoming message packets. The firewall accepts or denies access requests based on filtering rules that have been programmed into it. Network-level firewalls are insecure because they are designed to facilitate the free flow of information rather than restrict it. This method does not explicitly authenticate outside users.

Application-level firewalls – This type of firewalls provide a high level of customizable network security, but can be extremely expensive. These systems are configured to run security applications called proxies that permit routine services such as e-mail to pass

PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

through the firewall, but can perform sophisticated functions such as logging or user authentication for specific tasks. If an outside user attempts to connect to an unauthorized service or file, the network administrator or security group can be notified immediately.

Question 5

- (a) List out the important characteristics of useful and effective information. (6 Marks)
- (b) What are the four common cycles of business activity according to which transactions may be grouped? Also distinguish between a transaction file and a master file. (5 Marks)
- (c) What are the five concurrent audit techniques that IS auditors commonly use? (5 Marks)

Answer

- (a) Important characteristics of useful and effective information are listed below:
 1. *Timeliness*: Information to be of any use has to be timely.
 2. *Purpose*: Information must have purposes at the time it is transmitted to a person or machine.
 3. *Mode and format*: The modes of communication in business may be either visual, verbal or in written form. Format of information should be so designed that it assists in decision making, solving problems, initiating planning, controlling and searching.
 4. *Redundancy*: It means the excess of information carried per unit of data.
 5. *Rate*: The rate of transmission/reception of information may be represented by the time required to understand a particular situation.
 6. *Frequency*: The frequency with which information is transmitted or received affects its value.
 7. *Completeness*: The information should be as complete as possible.
 8. *Reliability*: In statistical surveys, for example, the information that is arrived at should have an indication of the confidence level.
 9. *Cost benefit Analysis*: The benefits that are derived from the information must justify the cost incurred in procuring information.
 10. *Validity*: It measures the closeness of the information to the purpose which it purports to serve.
 11. *Quality*: Quality refers to the correctness of information.
- (b) The four common cycles of business activity according to which transactions may be grouped, are given as under:
 - (i) **Revenue Cycle** - Events related to the distribution of goods and services to other entities and the collection of related payments;

FINAL (OLD) EXAMINATION : NOVEMBER, 2010

- (ii) **Expenditure Cycle** - Events related to the 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; and
- (iv) **Finance Cycle** - Events related to the acquisition and management of capital funds, including cash.

The major difference between a transaction file and a master file is that transaction files usually contain data that are of temporary interest, while master files contain data that are of a more permanent or continuing interest.

(c) Five concurrent audit techniques that IS auditors commonly use, are given as follows:

- (i) **Integrated Test Facility (ITF)** – Here, a small set of fictitious and actual records are processed together. The system must distinguish ITF records from actual records, collect information on the effects of 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.
- (ii) **The Snapshot technique** – In this technique, 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)** - It 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 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** - These are audit routines that flag suspicious transactions. When audit holds 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)** - It embeds an audit module in a DBMS. 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.

PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

Question 6

- (a) *Briefly discuss guidelines for presenting tabular and graphic information.* (6 Marks)
(b) *Discuss some of the destructive programs.* (5 Marks)
(c) *Enumerate the characteristics of Enterprise Resource Planning (ERP) Systems.* (5 Marks)

Answer

- (a) The guidelines for presenting tabular and graphical information are discussed as follows:

- 1. 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 application, but in general, we can list down the items that should be included in tabular outputs:

1. Exceptions to normal expectations;
2. Major categories or groups of activities or entities;
3. Summaries of major categories or activities;
4. Unique identification information; and
5. Time dependent entities.

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

- 2. 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 for the tabular and narrative forms of information display for detecting the 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.

- (b) Destructive programs such as viruses are responsible for huge amount of corporate losses annually. The losses are measured in terms of data corruption and destruction,

FINAL (OLD) EXAMINATION : NOVEMBER, 2010

degraded computer performance, hardware destruction, violations of privacy, and the personnel time devoted for repairing the damage. Some of the common types of destructive programs are discussed below:

1. **Virus:** A virus is a program (usually destructive) that attaches itself to a legitimate program to penetrate the operating system. The virus destroys application programs, data files, and operating systems in a number of ways. One common technique is for the virus to simply replicate itself over and over within the main memory, thus destroying whatever data or programs are resident. One of the most insidious aspects of a virus is its ability to spread throughout the system and to other systems before perpetrating its destructive acts. Typically, a virus will have a built-in counter that will inhibit its destructive role until the virus has copied itself a specified number of times to other programs and systems. The virus thus grows geometrically, which makes tracing its origin extremely difficult.

Virus programs usually attach themselves to the following types of files:

1. An .EXE or .COM program file
2. The .OVL (overlay) program file
3. The boot sector of a disk
4. A device driver program.

When a virus infected program is executed, the virus searches the system for uninfected programs and copies itself into these programs. The virus in this way spreads to the applications of other users or to the operating system itself.

2. **Worm:** The term worm is used interchangeably with virus. A worm is a software program that "burrows" into the computer's memory and replicates itself into areas of idle memory. The worm systematically occupies idle memory until the memory is exhausted and the system fails. Worms differ from viruses in that the replicated worm modules remain in contact with the original worm that controls their growth. The replicated virus modules, on the other hand, grow independently of the initial virus.
3. **Logic Bomb:** A logic bomb is a destructive program, such as a virus, that is triggered by some predetermined event. Quite often a date (such as Friday the 13TH, April fool's day, or a birthday) will be the logic bomb's trigger. The famous Michelangelo virus (triggered by his birth date) is an example of a logic bomb.
4. **Back Door:** A back door (also called a trap door) is a software program that allows unauthorized access to a system without going through the normal (front door) log-on procedure. Programmers, who want to provide themselves with unrestricted access to the programs that they are developing for users may create a long-on procedure that will accept both the user's private password and their own secret password, thus creating a back door to the system. The purpose of the back door may be to provide easy access to perform program maintenance, or it may be to perpetrate a fraud or insert a virus into the system.

PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

5. **Trojan Horse:** It is a program whose purpose is to capture Ids and passwords from unsuspecting users. The program is designed to mimic the normal log-in procedures of the operating system. When the user enters his/her ID and password, the Trojan horse stores a copy of them in a secret file. At some later date, the author of the Trojan horse uses these Ids and passwords to access the system and masquerade as an authorized user.

- (c) The characteristics of ERP systems are given as follows:

Flexibility: An ERP system should be flexible to respond to the changing needs of an enterprise. The client server technology enables ERP to run across various database back ends through Open Database Connectivity (ODBC).

Modular and Open: ERP system has to have open system architecture. This means that any module can be interfaced or detached whenever required without affecting the other modules. It should support multiple hardware platforms for the companies having heterogeneous collection of systems. It must support some the third party add-ons also.

Comprehensive: It should be able to support variety of organizational functions and must be suitable for a wide range of business organizations.

Beyond The Company: It should not be confined to the organizational boundaries, rather support the on-line connectivity to the other business entities of the organization.

Best Business Practices: It must have a collection of the best business processes applicable worldwide. An ERP package imposes its own logic on a company's strategy; culture and organization.

Question 7

Answer any **four**:

- (a) Discuss the various steps involved in system testing. (4 Marks)
- (b) What are the basic ground rules that must be addressed sequentially while protecting computer-held information? (4 Marks)
- (c) Give the four key components comprising the integrated environments formed by all dimensions of software engineering. (4 Marks)
- (d) What are the different aspects to be considered in Meta-CASE workbenches? (4 Marks)
- (e) Briefly describe the method of Business Engineering. (4 Marks)

Answer

- (a) Various steps involved in system testing are given as under:
- (i) Preparation of realistic test data in accordance with the system test plan;
 - (ii) Processing the test data, using the new equipment;
 - (iii) Thorough checking of the results of all system tests; and
 - (iv) Reviewing the results with future users, operators and support personnel.

FINAL (OLD) EXAMINATION : NOVEMBER, 2010

- (b) The basic ground rules that must be addressed sequentially, while protecting computers-held information are given as follows:

Rule (i) We need to know 'what the information is' and 'where it is located'.

Rule (ii) We need to know the value of the information held and how difficult it would be to recreate if it was damaged or lost.

Rule (iii) We need to know 'who is authorized to access the information' and 'what they are permitted to do with the information'.

Rule (iv) We need to know 'how quickly information needs to be made available', 'should it become unavailable for whatever reason (loss, unauthorized modification etc.)'

- (c) Four key components comprising the integrated environments formed by all dimensions of software engineering are given as follows:

(i) *Analysis Dimension* consisting of planning systems, defining requirements and designing systems.

(ii) *Development Dimension* consisting of traditional programming development tools like Editors, Compilers, Debuggers, Code and Application Generators.

(iii) *Management Dimension* providing methods and tools needed to manage and control projects.

(iv) *Support Dimension* comprising all tools and techniques needed to sustain and evolve existing software systems.

- (d) There are five different aspects, which are to be considered in Meta-CASE workbenches:

1. A data model for data capture and output generation.
2. A frame model, which defines the views of the data model to be generated. Each possible view of the data model is termed as frame. Links between frames, which allow navigation from one representation to another are defined in this model.
3. Diagrammatic notation for each diagram frame.
4. Textual presentation for each text frame.
5. Report structure.

(e) Business Engineering

- Business Engineering has come out of merging of two concepts namely Information Technology and Business Process Reengineering.
- Business Engineering is the rethinking of Business Processes to improve speed, quality and output of materials or services.
- The emphasis of business engineering is the concept of Process Oriented Business Solutions enhanced by the Client-Server computing in Information Technology.
- The main point in business engineering is the efficient redesigning of company's value added chains. Value added chains are a series of connected steps running

PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

through a business, which when efficiently completed, add value to enterprise and customers. Information technology helps to develop business models, which assist in redesigning of business processes.

- Business Engineering is the method of development of business process according to changing requirements.

