

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT QUESTIONS

Information Systems Concepts

1. (a) Define the following terms:
 - (i) Abstract System, (ii) Physical System, (iii) Entropy
- (b) Discuss different levels of management activities in management planning and control hierarchy.
2. (a) Describe the three levels of implementation of databases.
- (b) Discuss various business applications of Experts Systems.
3. (a) Explain Knowledge Acquisition Subsystem (KAS) in brief.
- (b) What is an Electronic Message Communication System? Discuss its components in detail.

Software Development Life Cycle Methodology

4. (a) Describe the reasons why organizations fail to achieve their systems development objectives.
- (b) Explain the strengths and weaknesses of the Waterfall model.
5. (a) What are the aspects that should be kept in mind while eliciting information to delineate the scope?
- (b) Discuss the areas which should be studied in depth, in order to fully understand the present system and its related problems.
6. (a) Explain the characteristics of a good coded program.
- (b) Describe various activities involved in conversion from previous system to the new information system.

Control Objectives

7. (a) Discuss IS Audits categorization in brief.
- (b) What do you understand by financial control techniques? Discuss a few examples of the same.
8. (a) What are the data processing controls? Explain in brief.
- (b) Discuss the controls and Auditor's role with respect to Application Software Acquisition/Selection Process.
9. (a) What are the general questions that the auditor will need to consider for quality control?
- (b) Explain data integrity policies in brief.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

Testing – General and Automated Controls

10. (a) What is a Unit Test Plan? Describe its various sections in brief.
- (b) What are the activities which should be performed by a reviewer, to test a physical security?

Risk Assessment Methodologies and Applications

11. (a) Briefly explain the risk management process.
- (b) Most qualitative risk analysis methodologies make use of a number of interrelated elements. What are those elements? Explain in brief.

Business Continuity Planning and Disaster Recovery Planning

12. (a) Discuss the objectives of performing BCP tests.
- (b) What are the areas which may be included in a disaster recovery and planning document?
13. (a) The most difficult part in preparing a backup plan is to ensure that all critical resources are backed up. Discuss the resources that must be considered in the same.
- (b) Describe various tasks covered under the second phase of developing a business continuity plan i.e. 'Vulnerability Assessment and definition of requirement'.

An Overview of Enterprise Resource Planning (ERP)

14. (a) XYZ Company developed an information system for the integration of various organizational processes. The company wanted to sell this system as an ERP solution. But, any system has to possess few characteristics to qualify for a true ERP solution. What are those characteristics? Explain in brief.
- (b) Describe the following processes in brief:
 - (i) Forecasting
 - (ii) Fund management
 - (iii) Price Planning
 - (iv) Budget Allocation
 - (v) Material requirement planning
 - (vi) Quality control
15. (a) Explain the useful tasks served by budgeting function, in brief.
- (b) There are certain general guidelines which are to be followed before starting the implementation of an ERP package. Briefly discuss those guidelines.

Information Systems Auditing Standards, Guidelines, Best Practices

FINAL (NEW) EXAMINATION : NOVEMBER, 2010

16. (a) Security policy involves a thorough understanding of the organization business goals and its dependence on information security. What are the areas which should be covered under this policy? Also mention its controls and objectives.
- (b) What is a maturity level of software process? Explain level 1 i.e. initial level maturity in detail.

17. (a) Discuss COBIT's working definitions in brief.
- (b) Explain the terms 'Software process capability' and 'Software process performance'.

Drafting of IS Security Policy, Audit Policy, IS Audit Reporting- A Practical Perspective

18. (a) State the major points that need to be taken into consideration in access control.
- (b) Give the contents of current file with respect to IS Audit working papers.

Information Technology (Amendment) Act 2008

19. (a) Define the following terms with respect to Information Technology (Amendment) Act, 2008:
 - (i) Computer Network
 - (ii) Electronic Signature
 - (iii) Electronic Signature Certificate
 - (iv) Intermediary
 - (v) Computer Source Code
 - (b) Discuss the Delivery of Services by Service Provider with respect to the Section 6A of Information Technology (Amendment) Act, 2008.
20. (a) Describe the punishment for sending offensive messages through communication service, etc. with respect to the Section 66A of Information Technology (Amendment) Act, 2008.
 - (b) Discuss National nodal agency with respect to the Section 70A of Information Technology (Amendment) Act, 2008.

Questions based on Case Studies

21. ABC Technologies Ltd. is in the development of application software for various domains. For the development purposes, the company is committed to follow the best practices suggested by SDLC. SDLC provides the guidelines in terms of a sequence of activities. It consists of a set of steps and phases in which each phase of the SDLC uses the results of the previous one. The SDLC is document driven which means that at crucial stages during the process, documentation is produced. A phase of the SDLC is not complete until the appropriate documentation or artifact is produced. These are sometimes referred to as deliverables.

A deliverable may be a substantial written document, a software artifact, a system test plan or even a physical object such as a new piece of technology that has been ordered

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

and delivered. This feature of the SDLC is critical to the successful management of an IS project.

Read the above carefully and answer the following:

- (a) List the possible advantages from the perspective of an IS Audit.
 - (b) There are various advantages by following SDLC, but there are some shortcomings also. Briefly explain those shortcomings.
 - (c) Feasibility study is a key activity in the SDLC. What are the issues which are typically considered in the Feasibility Study?
 - (d) At the end of the analysis phase of SDLC, the system analyst prepares a document called 'Systems Requirements Specifications (SRS)'. Briefly explain the contents of a SRS.
22. XYZ & Company is dealing in the information systems audit. The audit of an IS environment to evaluate the systems, practices and operations may include one or both of the following:
- Assessment of internal controls within the IS environment to assure validity, reliability, and security of information.
 - Assessment of the efficiency and effectiveness of the IS environment in economic terms.
- The IS audit process is to evaluate the adequacy of internal controls with regard to both specific computer programs and the data processing environment as a whole. This includes evaluating both the effectiveness and efficiency. The focus (scope and objective) of the audit process is not only on security which comprises confidentiality, integrity and availability but also on effectiveness (result-orientation) and efficiency (optimum utilization of resources).
- Read the above carefully and answer the following:
- (a) The audit objective and scope has a significant bearing on the skill and competence requirements of an IS auditor. There is a set of skills that is generally expected from an IS auditor. Discuss those skills in brief.
 - (b) Explain various costs involved in the implementation and operation of controls.
 - (c) Discuss the controls to consider when reviewing the organization and management controls in an Information System.
 - (d) While reviewing the adequacy of data security controls, what are the items which need to be evaluated by an IS auditor?
23. PQR Enterprises uses business continuity and disaster recovery plans in its various operations. Business continuity focuses on maintaining the operations of the organization, especially the IT infrastructure in face of a threat that has materialized. Disaster recovery, on the other hand, arises mostly when business continuity plan fails to

FINAL (NEW) EXAMINATION : NOVEMBER, 2010

maintain operations and there is a service disruption. This plan focuses on restarting the operation using a prioritized resumption list.

Read the above carefully and answer the following:

- (a) In your opinion, what should be the goals of a business continuity plan?
 - (b) In the development of a business continuity plan, there are total eight phases; Business Impact Analysis is the third important phase. Discuss various tasks which are to be undertaken in this phase.
 - (c) There are various backup techniques available e.g. Full backup, Incremental backup, Differential backup, and Mirror backup. Describe differential backup technique in detail.
24. RST Consultants is in the process of launching a new unit to provide various services to the organizations worldwide, to assist them right from the beginning i.e. from development to maintenance including strategic planning and e-governance areas. The company believes in the philosophy of green world i.e. uses papers to a minimum extent. COBIT is positioned to be comprehensive for management and to operate at a higher level than technology standards for information systems management. To satisfy business objectives, information needs to conform to certain criteria, which COBIT refers to as business requirements for information. In establishing the list of requirements, COBIT combines the principles embedded in existing and known reference models e. g. Quality Requirements, Fiduciary requirements, and Security Requirements.

Read the above carefully and answer the following:

- (a) Explain various working definitions of COBIT.
 - (b) Describe the IT resources identified in COBIT.
 - (c) Discuss the Monitoring domain identified for the high level classification in COBIT framework.
25. ABC Technologies is a leading company in the BPO sector. Its most of the business processes are automated. The company is relying on Information Technology for information and transaction processing. The growth of E-commerce supported by the growth of the Internet has completely revolutionized and reengineered business processes. The company's new business models and new methods presume that the information required by the business managers is available all the time; it is accurate, it is reliable and no unauthorized disclosure of the same is made. Further, it is also presumed that the virtual business organization is up and running all the time on 24×7 basis. However, in reality, the technology-enabled and technology-dependent organizations are more vulnerable to security threats than ever before.

Read the above carefully and answer the following:

- (a) Discuss the security objective of the organization.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- (b) There are certain basic ground rules that must be addressed sequentially, prior to knowing the details of 'how to protect the information systems'. Explain those rules in brief.
- (c) Describe various groups of management, comprised by security policy.

FINAL (NEW) EXAMINATION : NOVEMBER, 2010

SUGGESTED ANSWERS / HINTS

1. (a) (i) **Abstract System:** Abstract System also known as Conceptual System or Model, can be defined as an orderly arrangement of interdependent ideas or constructs. For example, a system of theology is an orderly arrangement of ideas about God and the relationship of humans to God.
 - (ii) **Physical System:** A physical system is a set of tangible elements which operate together to accomplish an objective. Some of its examples include: Circulatory System, Transportation System, Weapons System, School System, and Computer System.
 - (iii) **Entropy:** Entropy is the quantitative measure of disorder in a system. Systems can run down and decay or can become disordered or disorganized. Presenting or offsetting an increase in entropy requires inputs of matter and energy to repair, replenish and maintain the system. This maintenance input is termed as negative entropy. Open systems require more negative entropy than relatively closed systems for keeping at a steady state.
- (b) **Level of management activity:** Different levels of management activities in management planning and control hierarchy are Strategic level, Tactical level and Operational level.
- **Strategic Level or Top level:** Strategic level management is concerned with the developing of organizational mission, objectives and strategies. Decisions made at this level of organization to handle problems critical to the survival and success of the organization are called Strategic Decisions. They have a vital impact on the direction and functioning of the organization. For example - decisions on plant location, introduction of new products, making major new fund-raising and investment operations, adoption of new technology, acquisition of outside enterprises and so on are strategic decisions.
 - **Tactical Level or Middle level:** Tactical level lies in the middle of managerial hierarchy where managers plan, organize, lead and control the activities of other managers. Decisions made at this level, called the Tactical decisions (which are also called operational decisions), are made to implement strategic decisions. A single strategic decision calls for a series of tactical decisions, which are of a relatively structured nature. Tactical decisions are relatively short, step-like spot solutions to breakdown strategic decisions into implemental packages. Tactical decisions are specific and functional; made in a relatively closed setting; more easily available and digestible; and less surrounded by uncertainty and complexity.
 - **Operational level or Supervisory Level:** This is the lowest level in managerial hierarchy wherein the managers coordinate the work of others who are not themselves managers. They ensure that specific tasks are carried out effectively and efficiently.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

2. (a) **Implementation of Database :** Database is implemented at three levels as listed below:
- **Physical level:** It involves the implementation of the database on the hard disk i.e. storage of data in the hard disk. The management of storage and access is controlled by operating system.
 - **Logical Level:** It is designed by professional programmers, who have complete knowledge of DBMS. It deals with the nature of data stored, the scheme of the data, storage which is logically divided into various tables having rows and columns and the techniques for defining relationships with indexes.
 - **External level:** The logical level defines schema which is divided into smaller units known as sub-schemas and given to the managers, each sub-schema containing all relevant data needed by one manager.
- (b) Some of the business applications of Expert Systems are as follows:
- **Accounting and Finance:** It provides tax advice and assistance, helping with credit authorization decisions, selecting forecasting models, providing investment advice etc.
 - **Marketing:** It provides establishing sales quotas, responding to customer inquiries, referring problems to telemarketing centers, assisting with marketing timing decisions, determining discount policies etc.
 - **Manufacturing:** It helps in determining whether a process is running correctly, analyzing quality and providing corrective measures, maintaining facilities, scheduling job-shop tasks, selecting transportation routes, assisting with product design and faculty layouts.
 - **Personnel:** It is useful in assessing applicant qualifications, giving employees assisting at filling out forms.
 - **General Business:** It helps in assisting with project proposals, recommending acquisition strategies, educating trainees, evaluating performance etc.

3. (a) **Knowledge Acquisition Subsystem (KAS)**

The Knowledge Acquisition Subsystem is the software component of an Expert System that enables the Knowledge Engineer (KE), a specialized systems analyst responsible for designing and maintaining the expert System to build and refine an expert systems knowledge base. The KE works with the knowledge acquisition subsystem to model decision logic, derives industries and updates the knowledge base.

Knowledge base development and maintenance can be done using special, reasonably user-friendly software. This software provides a convenient and efficient means of capturing and storing the contents of the knowledge base. Users are often presented with easy-to-operate menus and templates for entering rules, facts and

FINAL (NEW) EXAMINATION : NOVEMBER, 2010

relationship among facts. Once these are entered, the software correctly stores the information in the knowledge base.

(b) Electronic Message Communication Systems

Business enterprises have been using a variety of electronic message communication systems for finding and receiving messages. These include telephone, mail and facsimile (Fax), etc. The computer based message communication systems offer a lot of economy not only in terms of reduced time in sending or receiving the message but also in terms of reliability of the message and cost of communication.

Components of Message Communication Systems

Three basic components of message communication systems are as follows:

(i) Electronic Mail: Various features of an electronic mail are stated below:

- **Electronic transmission:** The transmission of messages with email is electronic and message delivery is very quick, almost instantaneous. The confirmation of transmission is also quick and the reliability is very high.
- **Online development and editing:** The email message can be developed and edited online before transmission. The online development and editing eliminates the need for use of paper in communication. It also facilitates the storage of messages on magnetic media, thereby reducing the space required to store the messages.
- **Broadcasting and Rerouting:** Email permits sending a message to a large number of target recipients. Thus, it is easy to send a circular to all branches of a bank using Email resulting in a lot of saving of paper. The email could be rerouted to people having direct interest in the message with or without changing or and appending related information to the message.
- **Integration with other Information systems:** The E-mail has the advantage of being integrated with the other information systems. Such an integration helps in ensuring that the message is accurate and the information required for the message is accessed quickly.
- **Portability:** Email renders the physical location of the recipient and sender irrelevant. The email can be accessed from any personal computer equipped with the relevant communication hardware, software and link facilities.
- **Economical:** The advancements in communication technologies and competition among the communication service providers have made Email the most economical mode of sending messages. Since the speed of transmission is increasing, the time and cost on communication media per page is falling further, adding to the popularity of email. The email is

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

proving to be very helpful not only for formal communication but also for informal communication within the business enterprise.

(ii) Facsimile (Fax)

Facsimile (Fax) is electronic communication of images of documents over telephone lines. The computer based fax technology automates fax communication and permits sharing of fax facilities. It uses special software and fax servers to send and receive fax messages using common communication resources. These servers have the ability to receive fax messages and automatically reroute them to the intended recipient after viewing it at the central computer. Similarly, the managers in an enterprise can leave the fax messages to the server which will send it to the intended recipient automatically.

(iii) Voice Mail

Voice mail a variation of the email in which messages are transmitted as digitized voice. The recipient of the voice mail has to dial a voice mail service or access the e-mail box using the specified equipment and he can hear the spoken message in the voice of the sender. The secured type of voice mail service may require the recipient to enter identification code before the access is granted to the stored information.

4. (a) There are many reasons why organizations fail to achieve their systems development objectives. Some of them are as follows:

- **Lack of senior management support and involvement in information systems development:** Developers and users of information systems watch senior management to determine which systems development projects are important and act accordingly by shifting their efforts away from any project which is not receiving management attention. In addition, management can see that adequate resources, as well as budgetary control over use of those resources, are dedicated to the project.
- **Shifting user needs: User requirements for information technology are constantly changing.** As these changes accelerate, there will be more requests for systems development and more development projects. When these changes occur during a development process, the development team faces the challenge of developing systems whose very purposes might change since the development process began. Strategic decision making is unstructured, the requirements, specifications, and objectives for such development projects are difficult to define.
- **New technologies:** When an organization tries to create a competitive advantage by applying advance Information technology, it generally finds that attaining system development objectives is more difficult because personnel are not as familiar with the technology.

FINAL (NEW) EXAMINATION : NOVEMBER, 2010

- **Lack of standard project management and systems development methodologies:** Some organizations do not formalize their project management and system development methodologies, thereby making it very difficult to consistently complete projects on time or within budget.
- **Overworked or under-trained development staff:** In many cases, systems developers often lack sufficient education background. Furthermore, many companies do little to help their development personnel stay technically sound. Currently in these organizations, training plan and training budget do not exist.
- **Resistance to change:** People have a natural tendency to resist change, and information systems development projects signal changes - often radical - in the workplace. When personnel perceive that the project will result in personnel cutbacks, threatened personnel will dig in their heels, and the development project is doomed to failure.
- **Lack of user participation:** Users must participate in the development effort to define their requirements, feel ownership for project success, and work to resolve development problems. User participation also helps to reduce user resistance to change.
- **Inadequate testing and user training:** New systems must be tested before installation to determine that they operate correctly. Users must be trained to effectively utilize the new system.

To overcome these, organizations must execute the systems development process efficiently and effectively.

(b) Strengths of the Waterfall Model:

The major strengths of this model are given as follows:

- Ideal for supporting less experienced project teams and project managers or project teams whose composition fluctuates.
- An orderly sequence of development steps and design reviews ensure the quality, reliability, adequacy and maintainability of the developed software.
- Progress of system development is measurable.
- It conserves resources.

Weaknesses of the Waterfall Model:

The major weaknesses of this model are given as follows:

- Inflexible, slow, costly, and cumbersome due to significant structure and tight controls.
- Project progresses forward, with only slight movement backward.
- Little room for use of iteration, which can reduce manageability if used.
- Depends upon early identification and specification of requirements, yet users may not be able to clearly define what they need early in the project.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- Requirement inconsistencies, missing system components and unexpected development needs are often discovered during design and coding.
 - Problems are often not discovered until system testing.
 - System performance cannot be tested until the system is almost fully coded, and under capacity may be difficult to correct.
 - Difficult to respond to changes. Changes that occur later in the life cycle are more costly and are thus discouraged.
 - Produces excessive documentation and keeping it updated as the project progresses is time-consuming.
 - Written specifications are often difficult for users to read and thoroughly appreciate.
 - Promotes the gap between users and developers with clear vision of responsibility.
5. (a) While eliciting information to delineate the scope, major aspects that should be kept in mind, are stated as under:
- Different users will represent the problem and required solution in different ways. The system developer should elicit the need from the initiator of the project alternately called champion or executive sponsor of the project. Addressing his/her concerns should be the basis of the scope.
 - While the initiator of the project may be a member of the senior management, the actual users may be from the operating levels in an organization. An understanding of their profile helps in designing appropriate user interface features.
 - While presenting the proposed solution for a problem, the development organization has to clearly quantify the economic benefits to the user organization. The information required has to be gathered at this stage. For example - when a system is proposed for Road tax collection, data on the extent of collection and defaults is required to quantify benefits that will result to the Transport Department.
 - It is also necessary to understand the impact of the solution on the organization- its structure, roles and responsibilities. Solutions which have a wide impact are likely to meet with greater resistance. ERP implementation in organizations is a classic example of change management requirement. Organizations that have not been able to handle this have had a very poor ERP implementation record, with disastrous consequences.
 - While economic benefit is a critical consideration when deciding on a solution, there are several other factors that have to be given weightage too. These factors have to be considered from the perspective of the user management

FINAL (NEW) EXAMINATION : NOVEMBER, 2010

and resolved. For example, in a security system, how foolproof it is, may be a critical a factor like the economic benefits that entail.

- (b) In order to understand the present system and its related problems, the following areas should be studied in depth:

- **Review historical aspects:** A brief history of the organization is a logical starting point for an analysis of the present system. The historical facts should identify the major turning points and milestones that have influenced its growth. A review of annual reports and organization chart can identify the growth of management levels as well as the development of various functional areas and departments. The system analyst should investigate what system changes have occurred in the past including operations that have been successful or unsuccessful with computer equipments and techniques.
- **Analyze inputs:** A detailed analysis of present inputs is important since they are basic to the manipulation of data. Source documents are used to capture the originating data for any type of system. The system analyst should be aware of the various sources from where the data are initially captured, keeping in view the fact that outputs for one area may serve as an input for another area. The system analyst must understand the nature of each form, what is contained in it, who prepared it, from where the form is initiated, where it is completed, the distribution of the form and other similar considerations. If the analyst investigates these questions thoroughly, he will be able to determine how these inputs fit into the framework of the present system.
- **Review data files maintained:** The analyst should investigate the data files maintained by each department, noting their number and size, where they are located, who uses them and the number of times per given time interval these are used. Information on common data files and their size will be an important factor, which will influence the new information system. This information may be contained in the systems and procedures manuals. The system analyst should also review all on-line and off-line files which are maintained in the organization as it will reveal information about data that are not contained in any outputs. The related cost of retrieving and processing the data is another important factor that should be considered by the systems analyst.
- **Review methods, procedures and data communications:** Methods and procedures transform input data into useful output. A method is defined as a way of doing something; a procedure is a series of logical steps by which a job is accomplished. A procedure review is an intensive survey of the methods by which each job is accomplished, the equipment utilized and the actual location of the operations. Its basic objective is to eliminate unnecessary tasks or to perceive improvement opportunities in the present information system. A system analyst also needs to review and understand the present data communications used by the organization. He must review the types of data communication equipments including data interface, data links, modems, dial-

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

up and leased lines and multiplexers. The system analyst must understand how the data-communications network is used in the present system so as to identify the need to revamp the network when the new system is installed.

- **Analyze outputs:** The outputs or reports should be scrutinized carefully by the system analysts in order to determine how well they will meet the organization's needs. The analysts must understand what information is needed and why, who needs it and when and where it is needed. Additional questions concerning the sequence of the data, how often the form reporting is used, how long it is kept on file, etc. must be investigated. Often many reports are a carry-over from earlier days and have little relevance to current operations. Attempt should be made to eliminate all such reports in the new system.
- **Review internal controls:** A detailed investigation of the present information system is not complete until internal controls are reviewed. Locating the control points helps the analyst to visualize the essential parts and framework of a system. An examination of the present system of internal controls may indicate weaknesses that should be removed in the new system. The adoption of advanced methods, procedures and equipments might allow much greater control over the data.
- **Model the existing physical system and logical system:** As the logic of inputs, methods, procedures, data files, data communications, reports, internal controls and other important items are reviewed and analyzed in a top down manner; the process must be properly documented. The flow charting and diagramming of present information not only organizes the facts, but also helps disclose gaps and duplication in the data gathered. It allows a thorough comprehension of the numerous details and related problems in the present operation.
- **Undertake overall analysis of the present system:** Based upon the aforesaid investigation of the present information system, the final phase of the detailed investigation includes the analysis of the present work volume; the current personnel requirements; the present benefits and costs and each of these must be investigated thoroughly.

6. (a) A good coded program should have the following characteristics:

- **Reliability:** It refers to the consistency, which a program provides over a period of time. However poor setting of parameters could result in the failure of a program after some time.
- **Robustness:** It refers to the process of taking into account all possible inputs and outputs of a program in case of least likely situations.
- **Accuracy:** It refers not only to what program is supposed to do, but should also take care of what it should not do. The second part becomes more challenging for quality control personnel and auditors.

FINAL (NEW) EXAMINATION : NOVEMBER, 2010

- **Efficiency:** It refers to the performance which should not be unduly affected with the increase in input values.
 - **Usability:** It refers to a user-friendly interface and easy-to-understand document required for any program.
 - **Readability:** It refers to the ease of maintenance of program even in the absence of the program developer.
- (b) Conversion includes all those activities which must be completed to successfully convert from the previous system to the new information system. Fundamentally these activities can be classified as follows:
- (i) **Procedure conversion:** Operating procedures should be completely documented for the new system that applies to both computer-operations and functional area operations. Before any parallel or conversion activities can start, operating procedures must be clearly spelled out for personnel in the functional areas undergoing changes. Information on input, data files, methods, procedures, output, and internal controls must be presented in clear, concise and understandable terms for the average reader. Written operating procedures must be supplemented by oral communication during the training sessions on the system change.
 - (ii) **File conversion:** Because large files of information must be converted from one medium to another, this phase should be started long before programming and testing are completed. The cost and related problems of file conversion are significant whether they involve on-line files (common database) or off-line files. In order for the conversion to be as accurate as possible, file conversion programs must be thoroughly tested. Adequate controls, such as record counts and control totals, should be required output of the conversion program. The existing computer files should be kept for a period of time until sufficient files are accumulated for back up. This is necessary in case the files must be reconstructed from scratch after a "bug" is discovered later in the conversion routine.
 - (iii) **System conversion:** After on-line and off-line files have been converted and the reliability of the new system has been confirmed for a functional area, daily processing can be shifted from the existing information system to the new one. All transactions initiated after this time are processed on the new system. System development team members should be present to assist and to answer any questions that might develop. Consideration should be given to operating the old system for some more time to permit checking and balancing the total results of both systems.
 - (iv) **Scheduling personnel and equipment:** Scheduling data processing operations of a new information system for the first time is a difficult task for the system manager. As users become more familiar with the new system, the job becomes more routine. Schedules should be set up by the system

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

manager in conjunction with departmental managers of operational units serviced by the equipment. The master schedule for next month should provide sufficient computer time to handle all required processing.

7. (a) IT audits has been categorized into five types, as discussed below:

- **Systems and Applications:** An audit to verify that systems and applications are appropriate, are efficient, and are adequately controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity.
- **Information Processing Facilities:** An audit to verify that the processing facility is controlled to ensure timely, accurate, and efficient processing of applications under normal and potentially disruptive conditions.
- **Systems Development:** An audit to verify that the systems under development meet the objectives of the organization and to ensure that the systems are developed in accordance with generally accepted standards for systems development.
- **Management of IT and Enterprise Architecture:** An audit to verify that IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information processing.
- **Telecommunications, Intranets, and Extranets:** An audit to verify that controls are in place on the client (computer receiving services), server, and on the network connecting the clients and server.

(b) Financial Control Techniques

Financial controls are generally defined as the procedures exercised by the system user personnel over source, or transactions origination, documents before system input. These areas exercise control over transactions processing using reports generated by the computer applications to reflect un-posted items, non-monetary changes, item counts and amounts of transactions for settlement of transactions processed and reconciliation of the applications (subsystem) to general ledger. The financial control techniques are numerous. A few examples are highlighted here:

- **Authorization:** This entails obtaining the authority to perform some act typically access to such assets as accounting or application entries.
- **Budgets:** These estimates of the amount of time or money expected to be spent during a particular period of time, project, or event. The budget alone is not an effective control, budgets must be compared with the actual performance, including isolating differences and researching them for a cause and possible resolution.

FINAL (NEW) EXAMINATION : NOVEMBER, 2010

- **Cancellation of documents:** This technique marks a document in such a way to prevent its reuse. This is a typical control over invoices marking them with a "paid" or "processed" stamp or punching a hole in the document.
- **Documentation:** This includes written or typed explanations of actions taken on specific transactions; it also refers to written or typed instructions, which explain the performance of tasks.
- **Dual control:** This entails having two people simultaneously access an asset. For example, the depositories of banks' 24-hour teller machines should be accessed and emptied with two people present, many people confuse dual control with dual access, but these are distinct and different. Dual access divides the access function between two people: once access is achieved, only one person handles the asset. With teller-machines, for example, two tellers would open the depository vault door together, but only one would retrieve the deposit envelopes.
- **Input/ output verification:** This entails comparing the information provided by a computer system to the input documents. This is an expensive control that tends to be over recommended by auditors. It is usually aimed at such non-monetary by dollar totals and item counts.
- **Safekeeping:** This entails physically securing assets, such as computer disks, under lock and key, in a desk drawer, file cabinet storeroom, or vault.
- **Segregation of duties:** This entails assigning similar functions to separate people to provide reasonable assurance against fraud and provide an accuracy check of the other persons' work. For example, the responsibilities for making financial entries to the application and to the general ledger should be separated.
- **Sequentially numbered documents:** These are working documents with preprinted sequential numbers, which enable the detection of missing documents.
- **Supervisory review:** This refers to review of specific work by a supervisor but what is not obvious is that this control requires a sign-off on the documents by the supervisor, in order to provide evidence that the supervisor at least handled them. This is an extremely difficult control to test after the fact because the auditor cannot judge the quality of the review unless he or she witnesses it, and, even then, the auditor cannot attest to what the supervisor did when the auditor was not watching.

8. (a) Data processing controls are briefly discussed below:

- **Run-to-run totals:** These help in verifying data that is subject to process through different stages. If the current balance of an invoice ledger is Rs.150,000 and the additional invoices for the period is of total Rs.20,000 then the total sales value should be Rs.170,000. A specific record (probably the last record) can be used to maintain the control total.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- **Reasonableness verification:** Two or more fields can be compared and cross verified to ensure their correctness. For example, the statutory percentage of provident fund can be calculated on the gross pay amount to verify if the provident fund contribution deducted is accurate.
- **Edit checks:** Edit checks similar to the data validation controls can also be used at the processing stage to verify accuracy and completeness of data.
- **Field initialization:** Data overflow can occur if records are constantly added to a table or if fields are added to a record without initializing it, i.e., setting all values to zero before inserting the field or record.
- **Exception reports:** Exception reports are generated to identify errors in data processed. Such exception reports give the transaction code and why the particular transaction was not processed or what is the error in processing the transaction. For example, while processing a journal entry if only debit entry was updated and the credit entry was not updated due to absence of one of the important fields, then the exception report would detail the transaction code, and why it was not updated in the database.
- **Existence/Recovery Controls:** The check-point/restart logs facility is a short-term backup and recovery control that enables a system to be recovered if failure is temporary and localized.

(b) Application Software Acquisition/Selection Process

Once the information flow and processing within a system is identified and designed the application software may be acquired or developed in-house.

In case of acquisition of a software system, the following controls need to be in place:

- Information and system requirements need to meet business and system goals, system processes to be accomplished, and the deliverables and expectations for the system. The techniques include interviews, deriving requirements from existing systems, identifying characteristics from related system, and discovering them from a prototype or pilot system.
- A feasibility analysis to define the constraints or limitations for each alternative system from a technical as well as a business perspective. It should also include economic, technical, operational, schedule, legal or contractual, and political feasibility of the system within the organization scope.
- A detailed Request for Proposal (RFP) document needs to specify the acceptable requirements (functional, technical, and contractual) as well as the evaluation criteria used in the vendor selection process. The selection criteria should prevent any misunderstanding or misinterpretation.
- While identifying various alternatives, software acquisition involves the critical task of vendor evaluation. The vendor evaluation process considers the following:

FINAL (NEW) EXAMINATION : NOVEMBER, 2010

- ◆ Stability of the supplier company,
- ◆ Volatility of system upgrades,
- ◆ Existing customer base,
- ◆ Supplier's ability to provide support,
- ◆ Cost-benefits of the hardware/software in support of the supplier application, and
- ◆ Customized modifications of the application software.

Auditor's Role : Major roles of auditors are:

- To highlight risks before a vendor contract or a software agreement contract is signed.
 - To ensure that the decision to acquire software flows from the thorough feasibility study, vendor evaluation and RFP (Request for proposal) adequacy checked for.
 - A RFP would include transaction volume, data base size, turnaround time and response time requirements and vendor responsibilities.
 - The auditor needs to also check the criteria for pre-qualification of vendors and sufficient documentation available to justify the selection of the final vendor / product.
 - The auditor may also collect information through his own sources on vendor viability, support infrastructure, service record and the like.
 - Thorough review of the contract signed with the vendor for adequacy of safeguards and completeness. The contract should address the contingency plan in case of vendor failures such as, source code availability and third party maintenance support.
 - To ensure that the contract went through legal scrutiny before it was signed.
9. (a) The following are the general questions that the auditor will need to consider for quality control:
- Does the system design follow a defined and acceptable standard?
 - Have completed designs been discussed and agreed with the users?
 - Does the project's quality assurance procedures ensure that project documentation (e.g. design documents, specifications, test and installation plans) is reviewed against the organization's technical standards and policies, and the User Requirements Specification?
 - Do quality reviews follow a defined and acceptable standard?
 - Are quality reviews carried out under the direction of a technically competent person who is managerially independent from the design team?
 - Are auditors/security staffs invited to comment on the internal control aspects of system designs and development specifications?

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- Are statistics of defects uncovered during quality reviews and other forms of quality control maintained and analyzed for trends? Is the outcome of trend analysis fed back into the project to improve the quality of other deliverables?
- Are defects uncovered during quality reviews always corrected?
- Are all system resources (hardware, software, documentation) that have passed quality review been placed under change control management and version control?
- Has a System Installation Plan been developed and quality reviewed?
- Has a Training Plan been developed and quality reviewed? Has sufficient time and resources been allocated to its delivery? (to avoid “skills stagnation”, the delivery of training will need to be carefully scheduled).

(b) Data Integrity Policies

Various Data Integrity Policies are given as follows:

- **Virus-Signature Updating:** Virus signatures must be updated immediately when they are made available from the vendor.
- **Software Testing:** All software must be tested in a suitable test environment before installation on production systems.
- **Division of Environments:** The division of environments into Development, Test, and Production is required for critical systems.
- **Version Zero Software:** Version zero software (1.0, 2.0, and so on) must be avoided whenever possible to avoid undiscovered bugs.
- **Offsite Backup Storage:** Backups older than one month must be sent offsite for permanent storage.
- **Quarter-End and Year-End Backups:** Quarter-end and year-end backups must be done separately from the normal schedule, for accounting purposes.
- **Disaster Recovery:** A comprehensive disaster-recovery plan must be used to ensure continuity of the corporate business in the event of an outage.

10. (a) **Unit Test Plan:** The unit test plan is the overall plan to carry out the unit test activities. The lead tester prepares it and it is distributed to the individual testers. It contains the following sections:

- **What is to be tested?** The unit test plan must clearly specify the scope of unit testing. In this, normally the basic input/output of the units along with their basic functionality will be tested. The input units will mostly be tested for the format, alignment, accuracy and the totals. The UTP will clearly give the rules of what data types are present in the system, their format and their boundary conditions. This list may not be exhaustive; but it is better to have a complete list of these details.

FINAL (NEW) EXAMINATION : NOVEMBER, 2010

- **Sequence of Testing:** The sequences of test activities that are to be carried out in this phase are to be listed in this section. This includes, whether to execute positive test cases first or negative test cases first, to execute test cases based on the priority, to execute test cases based on test groups etc. Positive test cases prove that the system performs what is supposed to do; negative test cases prove that the system does not perform what it is not supposed to do. Testing the screens, files, database etc., are to be given in proper sequence.
- **Basic Functionality of Units:** How the independent functionalities of the units are tested which excludes any communication between the unit and other units. The interface part is out of scope of this test level. Apart from the above sections, the following sections are addressed, very specific to unit testing:
 - ◆ Unit Testing Tools,
 - ◆ Priority of Program units,
 - ◆ Naming convention for test cases,
 - ◆ Status reporting mechanism, and
 - ◆ Regression test approach.

(b) To test physical security, a reviewer should perform the following:

- Inspect the LAN wiring closet and transmission wiring and verify they are physically secured.
- Observe the LAN file server computer and verify it is secured in a manner to reduce the risk of removal of components and the computer itself.
- Obtain a copy of the key logs for the file server room and the wiring closet, match the key logs to actual keys that have been issued and determine that all keys held are assigned to the appropriate people, for example, the LAN Administrator and support staff.
- Select a sample of keys held by people without authorized access to the LAN file server facility and wiring closet and determine that these keys do not permit access to these facilities.
- Look for LAN operating manuals and documentation not properly secured.
- Environmental controls for LANs are similar to those considered in the mainframe environment. However, the equipment may not require as extensive atmospheric controls as a mainframe. The following should be considered:
 - ◆ LAN file server equipment should be protected from the effects of static electricity (antistatic rug) and electrical surges (surge protector)
 - ◆ Air conditioning and humidity control systems should be adequate to maintain temperatures within manufacturers' specifications.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- ◆ The LAN should be equipped with an uninterrupted power supply (UPS) that will allow the LAN to operate in case of minor power fluctuations or in case of a prolonged power outage.
- ◆ The LAN file server facility should be kept free of dust, smoke and other matter particularly food.
- ◆ Backup diskettes and tapes should be protected from environmental damage and the effects of magnetic fields.

11. (a) **Risk Management Process** : The broad process of risk management will be as follows:

1. Identify the technology related risks under the scope of operational risks.
2. Assess the identified risks in terms of probability and exposure.
3. Classify the risks as systematic and unsystematic.
4. Identify various managerial actions that can reduce exposure to systematic risks and the cost of implementing the same.
5. Look out for technological solutions available to mitigate unsystematic risks.
6. Identify the contribution of the technology in reducing the overall risk exposure. The analysis should not be restricted to the instant area of application of the technology but should be extended across the entire organization. This is necessary since many technologies may mitigate a specific type of risk but can introduce other kinds of risks.
7. Evaluate the technology risk premium on the available solutions and compare the same with the possible value of loss from the exposure.
8. Match the analysis with the management policy on risk appetite and decide on induction of the same.

(b) These elements are as under:

- Threats: These are things that can go wrong or that can 'attack' the system. Examples, might include fire or fraud. Threats are ever present for every system.
- Vulnerabilities: These make a system more prone to attack by a threat or make an attack more likely to have some success or impact. For example, for fire, vulnerability would be the presence of inflammable materials (e.g. paper).
- Controls: These are the countermeasures for vulnerabilities. There are four types of controls:
 - i) Deterrent controls reduce the likelihood of a deliberate attack,
 - ii) Preventative controls protect vulnerabilities and make an attack unsuccessful or reduce its impact,

FINAL (NEW) EXAMINATION : NOVEMBER, 2010

- iii) Corrective controls reduce the effect of an attack, and
iv) Detective controls discover attacks and trigger preventative or corrective controls.
- 12. (a)** The objectives of performing BCP tests are to ensure that:
- the recovery procedures are complete and workable,
 - the competence of personnel in their performance of recovery procedures can be evaluated,
 - the resources such as business processes, IS systems, personnel, facilities and data are obtainable and operational to perform recovery processes,
 - the manual recovery procedures and IT backup system/s are current and can either be operational or restored, and
 - the success or failure of the business continuity training program is monitored.
- (b)** The disaster recovery and planning document may include the following areas:
- The conditions for activating the plans, which describe the process to be followed before each plan, are activated.
 - Emergency procedures, which describe the actions to be taken following an incident which jeopardises business operations and/or human life. This should include arrangements for public relations management and for effective liaison with appropriate public authorities e.g. police, fire, services and local government.
 - Fallback procedures which describe the actions to be taken to move essential business activities or support services to alternate temporary locations, to bring business process back into operation in the required time-scale.
 - Resumption procedures, which describe the actions to be taken to return to normal business operations.
 - A maintenance schedule, which specifies how and when the plan will be tested, and the process for maintaining the plan.
 - Awareness and education activities, which are designed to create an understanding of the business continuity, process and to ensure that the business continues to be effective.
 - The responsibilities of individuals describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.
 - Contingency plan document distribution list.
 - Detailed description of the purpose and scope of the plan.
 - Contingency plan testing and recovery procedure.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- List of vendors doing business with the organization, their contact numbers and address for emergency purposes.
 - Checklist for inventory taking and updating the contingency plan on a regular basis.
 - List of phone numbers of employees in the event of an emergency.
 - Emergency phone list for fire, police, hardware, software, suppliers, customers, back-up location, etc.
 - Medical procedure to be followed in case of injury.
 - Back-up location contractual agreement, correspondences etc.
 - Insurance papers and claim forms.
 - Primary computer centre hardware, software, peripheral equipment and software configuration.
 - Location of data and program files, data dictionary, documentation manuals, source and object codes and back-up media.
 - Alternate manual procedures to be followed such as preparation of invoices.
 - Names of employees trained for emergency situation, first aid and life saving techniques.
 - Details of airlines, hotels and transport arrangements.
13. (a) The following resources must be considered:
- **Personnel:** Training and rotation of duties among information system staff to enable them to replace others when required. Arrangements with another company for provision of staff.
 - **Hardware:** Arrangements with another company for provision of hardware.
 - **Facilities:** Arrangements with another company for provision of facilities.
 - **Documentation:** Inventory of documentation stored securely on-site and off-site.
 - **Supplies:** Inventory of critical supplies stored securely on-site and off-site with a list of vendors who provide all supplies.
 - **Data / information:** Inventory of files stored securely on site and off site.
 - **Applications software:** Inventory of application software stored on site and off site.
 - **System software:** Inventory of system software stored securely on site and off site.
- (b) This phase will include the following tasks:

FINAL (NEW) EXAMINATION : NOVEMBER, 2010

- (i) A thorough Security Assessment of the system and communications environment including personnel practices; physical security; operating procedures; backup and contingency planning; systems development and maintenance; database security; data and voice communications security; systems and access control software security; insurance; security planning and administration; application controls; and personal computers.
 - (ii) The Security Assessment will enable the business continuity team to improve any existing emergency plans and disaster prevention measures and to implement required emergency plans and disaster prevention measures where not in place.
 - (iii) Present findings and recommendations resulting from the activities of the Security Assessment to the Steering Committee so that corrective actions can be initiated in a timely manner.
 - (iv) Define the scope of the planning effort.
 - (v) Analyze, recommend and purchase recovery planning and maintenance software required to support the development and maintenance of the plans.
 - (vi) Develop a Plan Framework.
 - (vii) Assemble business continuity team and conduct awareness sessions.
14. (a) These characteristics 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 & 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 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.
- (b) (i) **Forecasting:** It shows sales, Fund Flows etc over a long period of time, say next two years.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- (ii) **Fund Management:** This is the necessity of funds and the way to raise these funds. Uncertainty and Risk factors are also to be considered. Simulation with 'What if' type analysis may be done.
 - (iii) **Price Planning:** It determines the price at which products are offered. It involves application of technology to pricing support such as commercial database services along with feedback and sensitivity analysis.
 - (iv) **Budget Allocation:** Using computerized algorithms to estimate desirable mix of funds allocated to various functions is called budget allocation.
 - (v) **Material Requirement Planning:** This takes care of the process of making new products from raw materials and include production scheduling, requirement planning. It also includes activities for monitoring and planning of actual production.
 - (vi) **Quality Control:** It takes care of activities to ensure that the products are of desired quality.
15. (a) Budgeting function serves many useful functions such as:
- Original Budget approval and release,
 - Budget supplements, returns, transfers,
 - Fund centers and their hierarchical structures provide a base for top down budgeting and represent responsibility areas within the budget control.
 - Commitment management system enables to control various funds commitments and determine how much of the budget has already been utilized via availability checking. The information system can supply information at any time depending on when, where and how the funds commitment arose.
 - Analyses by responsibility area and commitment items allow identification of any budget bottlenecks.
- (b) The guidelines which should be followed before starting the implementation of ERP are stated below:
- Understanding the corporate needs and culture of the organization and then adopting the implementation technique to match these factors.
 - Doing a business process redesign exercise prior to starting the implementation.
 - Establishing a good communication network across the organization.
 - Providing a strong and effective leadership so that people down the line are well motivated.
 - Finding an efficient and capable project manager.
 - Creating a balanced team of implementation consultants who can work together as a team.

FINAL (NEW) EXAMINATION : NOVEMBER, 2010

- Selecting a good implementation methodology with minimum customization.
 - Training end users.
 - Adapting the new system and making the required changes in the working environment to make effective use of the system in future.
16. (a) The security policy should cover the following:
- a definition of information security,
 - a statement of management intention supporting the goals and principles of information security,
 - allocation of responsibilities for every aspect of implementation,
 - an explanation of specific applicable proprietary and general principles, standards and compliance requirements,
 - an explanation of the process for reporting of suspected security incidents,
 - a defined review process for maintaining the policy document,
 - means for assessing the effectiveness of the policy embracing cost and technological changes, and
 - nomination of the policy owner.
- The detailed control and objectives are as follows:
- **Information Security Policy:** To provide management direction and support for information security,
 - **Information System Infrastructure:** To manage information security within the organization,
 - **Security of third party access:** To maintain the security of organizational information processing facilities and information assets accessed by third parties, and
 - **Outsourcing:** To maintain the security of information when the responsibility for information processing has been outsourced to another organization.
- (b) A maturity level is a well-defined evolutionary level toward achieving a mature software process. Each maturity level comprises a set of process goals that, when satisfied, stabilize an important component of the software process. Achieving each level of the maturity framework establishes a different component in the software process, resulting in an increase in the process capability of the organization.
- CMM has total five levels, given as follows:
- Level 1: The Initial Level,
 - Level 2: The Repeatable Level,
 - Level 3: The Defined Level,

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- Level 4: The Managed Level, and
- Level 5: The Optimizing Level.

Level 1: The Initial Level: At the Initial Level, the organization typically does not provide a stable environment for developing and maintaining software. Such organizations frequently have difficulty making commitments that the staff can meet with an orderly engineering process, resulting in a series of crises. During a crisis, projects typically abandon planned procedures and revert to coding and testing. Success depends entirely on having an exceptional manager and a seasoned and effective software team. Occasionally, capable and forceful software managers can withstand the pressures to take shortcuts in the software process; but when they leave the project, their stabilizing influence leaves with them. Even a strong engineering process cannot overcome the instability created by the absence of sound management practices. In spite of this adhoc, even chaotic, process, Level 1 organizations frequently develop products that work, even though they may be over the budget and schedule. Success in Level 1 organizations depends on the competence and heroics of the people in the organization and cannot be repeated unless the same competent individuals are assigned to the next project. Thus, at Level 1, capability is a characteristic of the individuals, not of the organization.

17. (a) COBIT's working definitions are as follows:

- **Effectiveness:** It deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.
- **Efficiency:** It concerns the provision of information through the optimal (most productive and economical) use of resources.
- **Confidentiality:** It concerns the protection of sensitive information from unauthorized disclosure.
- **Integrity:** It relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.
- **Availability:** It relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.
- **Compliance:** It deals with complying with those laws, regulations and contractual arrangements to which the business process is subjected, i.e., externally imposed business criteria.
- **Reliability of Information:** It relates to the provision of appropriate information for management to operate the entity and for management to exercise its financial and compliance reporting responsibilities.

(b) **Software process capability:** It describes the range of expected results that can be achieved by following a software process. The software process capability of an

FINAL (NEW) EXAMINATION : NOVEMBER, 2010

organization provides one means of predicting the most likely outcomes to be expected from the next software project the organization undertakes.

Software process performance: It represents the actual results achieved by following a software process. Thus, software process performance focuses on the results achieved, while software process capability focuses on results expected.

18. (a) In Access Control, the following points need to be taken into consideration:

- Access controls must be in place to prevent unauthorized access to information systems and computer applications.
- Access must only be granted in response to a business requirement. Formal processes must be in place to provide individuals with access. The requirement for access must be reviewed regularly.
- System Owners are responsible for approving access to systems and they must maintain records of who has access to a particular system and at what level. The actual access controls in place must be audited against this record on a regular basis.
- Users should be granted access to systems only up to the level required to perform their normal business functions.
- The registration and de-registration of users must be formally managed.
- Access rights must be deleted for individuals who leave or change jobs.
- Each individual user of an information system or computer application will be provided with a unique user identifier (user id).
- It should not be permitted for an individual to use another person's user id or to log-on, to allow another individual to gain access to an information system or computer application.
- PCs and terminals should never be left unattended whilst they are connected to applications or the network. Someone may use the equipment to access confidential information or make unauthorized changes.
- Passwords Policy should be defined and the structure of passwords and the duration of the passwords should be specified. Passwords must be kept confidential and never disclosed to others.
- Mobile computing - When using mobile computing facilities, such as laptops, notebooks, etc., special care should be taken to ensure that business information is not compromised, particularly when the equipment is used in public places.

(b) The current file normally includes:

- Correspondence relating to the acceptance of appointment and the scope of the work,
- Evidence of the planning process of the audit and audit programme,

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- A record of the nature, timing, and extent of auditing procedures performed, and the results of such procedures,
- Copies of letters and notes concerning audit matters communicated to or discussed with the client, including material weaknesses in relevant internal controls,
- Letters of representation and confirmation received from the client,
- Conclusions reached by the auditor concerning significant aspects of the audit, including the manner in which the exceptions and unusual matters, if any, disclosed by the auditor's procedures were resolved and treated, and
- Copies on the data and system being reported on and the related audit reports.

- 19. (a) (i)** **Computer Network:** "Computer Network" means the interconnection of one or more Computers or Computer systems or Communication device through-
- (i) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and
 - (ii) terminals or a complex consisting of two or more interconnected computers or communication device whether or not the interconnection is continuously maintained;
- (ii)** **Electronic Signature:** "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.
- (iii)** **Electronic Signature Certificate:** "Electronic Signature Certificate" means an Electronic Signature Certificate issued under section 35 and includes Digital Signature Certificate".
- (iv)** **Intermediary:** "Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes.
- (v)** **Computer Source Code:** "Computer Source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.
- (b) [Section 6A] Delivery of Services by Service Provider (Inserted vide ITAA-2008):**
- (1) The appropriate Government may, for the purposes of this Chapter and for efficient delivery of services to the public through electronic means authorize, by order, any service provider to set up, maintain and upgrade the

FINAL (NEW) EXAMINATION : NOVEMBER, 2010

computerized facilities and perform such other services as it may specify, by notification in the Official Gazette.

Explanation: For the purposes of this section, service provider so authorized includes any individual, private agency, private company, partnership firm, sole proprietor form or any such other body or agency which has been granted permission by the appropriate Government to offer services through electronic means in accordance with the policy governing such service sector.

- (2) The appropriate Government may also authorize any service provider authorized under sub-section (1) to collect, retain and appropriate service charges, as may be prescribed by the appropriate Government for the purpose of providing such services, from the person availing such service.
- (3) Subject to the provisions of sub-section (2), the appropriate Government may authorize the service providers to collect, retain and appropriate service charges under this section notwithstanding the fact that there is no express provision under the Act, rule, regulation or notification under which the service is provided to collect, retain and appropriate e-service charges by the service providers.
- (4) The appropriate Government shall, by notification in the Official Gazette, specify the scale of service charges which may be charged and collected by the service providers under this section:

Provided that the appropriate Government may specify different scale of service charges for different types of services.

20. (a) [Section 66 A] Punishment for sending offensive messages through communication service, etc.:

Any person who sends, by means of a computer resource or a communication device,-

- (a) any information that is grossly offensive or has menacing character; or
- (b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently by making use of such computer resource or a communication device,
- (c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages (Inserted vide ITAA 2008) shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation: For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

(b) [Section 70 A] National nodal agency. (Inserted vide ITAA 2008):

- (1) The Central Government may, by notification published in the official Gazette, designate any organization of the Government as the national nodal agency in respect of Critical Information Infrastructure Protection.
- (2) The national nodal agency designated under sub-section (1) shall be responsible for all measures including Research and Development relating to protection of Critical Information Infrastructure.
- (3) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.

21. (a) From the perspective of the IS Audit, the following are the possible advantages:

- The IS auditor can have clear understanding of the various phases of the SDLC on the basis of the detailed documentation created during each phase of the SDLC.
- The IS Auditor on the basis of his examination, can state in his report about the compliance by the IS management of the procedures, if any, set by the management.
- The IS Auditor, if has a technical knowledge and ability of the area of SDLC, can be a guide during the various phases of SDLC.
- The IS auditor can provide an evaluation of the methods and techniques used through the various development phases of the SDLC.

(b) Some of the shortcomings of the SDLC are as follows:

- The development team may find it cumbersome.
- The users may find that the end product is not visible for a long time.
- The rigidity of the approach may prolong the duration of many projects.
- IT may not be suitable for small and medium sized projects.

(c) The following issues are typically addressed in the Feasibility Study:

- Determine whether the solution is as per the business strategy.
- Determine whether the existing system can rectify the situation without a major modification.
- Define the time frame for which the solution is required.
- Determine the approximate cost to develop the system.
- Determine whether the vendor product offers a solution to the problem.

(d) Any SRS contains the following:

FINAL (NEW) EXAMINATION : NOVEMBER, 2010

- **Introduction:** Goals and Objectives of the software context of the computer-based system; Information description.
 - **Information Description:** Problem description; Information content, flow and structure; Hardware, software, human interfaces for external system elements and internal software functions.
 - **Functional Description:** Diagrammatic representation of functions; Processing narrative for each function; Interplay among functions; Design constraints.
 - **Behavioral Description:** Response to external events and internal controls.
 - **Validation Criteria:** Classes of tests to be performed to validate functions, performance and constraints.
 - **Appendix:** Data flow / Object Diagrams; Tabular Data; Detailed description of algorithms charts, graphs and other such material.
 - **SRS Review:** It contains the following :
 - ◆ The development team makes a presentation and then hands over the SRS document to be reviewed by the user or customer.
 - ◆ The review reflects the development team's understanding of the existing processes. Only after ensuring that the document represents existing processes accurately, should the user sign the document. This is a technical requirement of the contract between users and development team / organization.
- 22. (a)** The set of skills that is generally expected from an IS auditor, include:
- Sound knowledge of business operations, practices and compliance requirements,
 - Should possess the requisite professional technical qualification and certifications,
 - A good understanding of information Risks and Controls,
 - Knowledge of IT strategies, policy and procedure controls,
 - Ability to understand technical and manual controls relating to business continuity, and
 - Good knowledge of Professional Standards and Best practices of IT controls and security.
- (b)** Implementing and operating controls in a system involves the following five costs:
- **Initial setup cost:** This cost is incurred to design and implement controls. For example, a security specialist must be employed to design a physical security system.
 - **Executing cost:** This cost is associated with the execution of a control. For example, the cost incurred in using a processor to execute input validation routines for a security system.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- **Correction costs:** The control has operated reliably in signaling an error or irregularity, the cost associated with the correction of error or irregularity.
 - **Failure cost:** The control malfunctions or not designed to detect an error or irregularity. These undetected or uncorrected errors cause losses.
 - **Maintenance costs:** The cost associated in ensuring the correct working of a control. For example, rewriting input validation routines as the format of input data changes.
- (c) The controls to consider while reviewing the organization and management controls in an Information system shall include:
- **Responsibility:** The strategy to have a senior management personnel responsible for the IS within the overall organizational structure.
 - **An official IT structure:** There should be a prescribed organization structure with all staff deliberated on their roles and responsibilities by written down and agreed job descriptions.
 - **An IT steering committee:** The steering committee shall comprise of user representatives from all areas of the business, and IT personnel. The committee would be responsible for the overall direction of IT. Here the responsibility lies beyond just the accounting and financial systems, for example, the telecommunications system (phone lines, video-conferencing) office automation, and manufacturing processing systems.
- (d) An IS auditor is responsible to evaluate the following while reviewing the adequacy of data security controls:
- Who is responsible for the accuracy of the data?
 - Who is permitted to update data?
 - Who is permitted to read and use the data?
 - Who is responsible for determining who can read and update the data?
 - Who controls the security of the data?
 - If the IS system is outsourced, what security controls and protection mechanism does the vendor have in place to secure and protect data?
 - Contractually, what penalties or remedies are in place to protect the tangible and intangible values of the information?
 - The disclosure of sensitive information is a serious concern to the organization and is mandatory on the auditor's list of priorities.
23. (a) The goals of a business continuity plan should be to:
- identify weaknesses and implement a disaster prevention program;
 - minimize the duration of a serious disruption to business operations;

FINAL (NEW) EXAMINATION : NOVEMBER, 2010

- facilitate effective co-ordination of recovery tasks; and
 - reduce the complexity of the recovery effort.
- (b) A number of tasks are to be undertaken in this phase are given as follows:
- Identify organizational risks - This includes single point of failure and infrastructure risks. The objective is to identify risks and opportunities and to minimize potential threats that may lead to a disaster.
 - Identify critical business processes.
 - Identify and quantify threats/ risks to critical business processes both in terms of outage and financial impact.
 - Identify dependencies and interdependencies of critical business processes and the order in which they must be restored.
 - Determine the maximum allowable downtime for each business process.
 - Identify the type and the quantity of resources required for recovery e.g. tables chairs, faxes, photocopies, safes, desktops, printers, etc.
 - Determine the impact to the organization in the event of a disaster, e.g. financial reputation, etc.

- (c) **Differential Backup:** A differential backup stores files that have changed since the last full backup. Therefore, if a file is changed after the previous full backup, a differential backup takes less time to complete than a full back up. Comparing with full backup, differential backup is obviously faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved.

Restoring from a differential backup is a two-step operation: Restoring from the last full backup; and then restoring the appropriate differential backup. The downside to using differential backup is that each differential backup will probably include files that were already included in earlier differential backups.

24. (a) COBIT's working definitions are as follows:

- **Effectiveness:** It deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.
- **Efficiency:** It concerns the provision of information through the optimal (most productive and economical) use of resources.
- **Confidentiality:** It concerns the protection of sensitive information from unauthorized disclosure.
- **Integrity:** It relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- **Availability:** It relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.
 - **Compliance:** It deals with complying with those laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria.
 - **Reliability of Information:** It relates to the provision of appropriate information for management to operate the entity and for management to exercise its financial and compliance reporting responsibilities.
- (b) The IT resources identified in COBIT can be explained / defined as follows:
- **Data:** These are objects in their widest sense (i.e. external and internal), structured and nonstructured, graphics, sound, etc.
 - **Application systems:** These are understood to be the sum of manual and programmed procedures.
 - **Technology:** It covers hardware, operating systems, database management systems, networking, multimedia, etc.
 - **Facilities:** These are all the resources to house and support information systems.
 - **People:** It includes staff skills, awareness and productivity to plan, organize, acquire, deliver, support and monitor information systems and services.
- (c) **Monitoring:** All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain thus addresses management's oversight of the organization's control process and independent assurance provided by internal and external audit or obtained from alternative sources.

The following table lists the high level control objectives for the Monitoring domain.

Entire top and middle tiers of COBIT:

Monitor and Evaluate

ME1	Monitor and Evaluate IT Processes
ME2	Monitor and Evaluate Internal Control
ME3	Ensure Regulatory Compliance
ME4	Provide IT Governance

25. (a) **Security Objective :** The objective of information system 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 confidentiality, integrity, and availability”.

FINAL (NEW) EXAMINATION : NOVEMBER, 2010

For any organization, the security objective comprises three universally accepted attributes:

- **Confidentiality:** Prevention of the unauthorized disclosure of information.
- **Integrity:** Prevention of the unauthorized modification of information.
- **Availability:** Prevention of the unauthorized withholding of information.

The relative priority and significance of confidentiality, integrity and availability vary according to the data within the information system and the business context in which it is used.

(b) Prior to knowing the details of 'how to protect the information systems', we need to define a few basic ground rules that must be addressed sequentially. These rules are:

- **Rule #1:** We need to know that 'what the information systems are' and 'where these are located'.
- **Rule #2:** We need to know the value of the information held and how difficult it would be to recreate if it were damaged or lost.
- **Rule #3:** We need to know that 'who is authorized to access the information' and 'what they are permitted to do with the information'.
- **Rule #4:** We need to know that 'how quickly information needs to be made available should it become unavailable for whatever reason (loss, unauthorized modification, etc.)'

(c) Security has to encompass managerial, technological and legal aspects. Security policy broadly comprises the following three groups of management:

- Management members who have budget and policy authority,
- Technical group who know what can and cannot be supported, and
- Legal experts who know the legal ramifications of various policy changes.

Information security policies must always take into account business requirements. Business requirements are the principles and objectives adopted by an organization to support its operations and information processing. E-commerce security is an example of such business requirements.

Furthermore, policies must consistently take into account the legal, statutory, regulatory and contractual requirements that the organization and its professional partners, suppliers and service providers must respect. The respect of intellectual property is a good example of such requirements.